IN THIS ISSUE >>> #38

Main Article:
Equifax Data Breach

Main Article Continued:
Equifax Data Breach

The Easy Button:
Freezing Your Credit

Bonus Materials:
Your Facebook Account

Update Corner:
Website Updates

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

CURRENT TOPICS >>>

DHS vs. Kaspersky Lab: Why the US government is ditching the Russian software giant
-Fox News

Three Equifax Managers Sold Stock Before Cyber Hack Revealed
-Bloomberg

Equifax Had Patch 2 Months Before Hack and Didn't Install It, Security Group Says
-USA Today

CURRENT COURSES >>>

ESSR

The Electronic Security and Signature Reduction (ESSR) course teaches students how to evaluate, manage and eliminate their digital signature. Students will learn how to secure data at rest and data in motion through open source programs and phone applications. Students will leave knowing how to "research" themselves and understand what the Internet has on their life. They will then learn how to manage or eliminate their online profile.

Equifax Data Breach

What you need to know

The term un-hackable does not exist in any context and this extends to credit bureaus. With the amount of information that credit bureaus hold on you, you would expect that their security would be top-notch and the way they handle data breaches would be open and pure in intentions. Enter in Equifax with one of the worst data breaches to date and the poorest way a company their size could handle it.

Back in March, a vulnerability was discovered in one of the most popular web server software: Apache. It was a very bad vulnerability which basically gave an attacker full access to any server running Apache Struts. The vulnerability was disclosed and 24 hours later a patch was issued to fix the vulnerability. Thanks to the quick response time of the Apache Software Foundation, companies had a patch and no one had to worry about some rogue hacker exploiting their web servers. That is if everyone installed the updates that they were supposed to. Nearly two months later, an attacker exploited the same vulnerability and gained access to Equifax's servers. Equifax believes the attackers had access for a month before they discovered someone had unauthorized access on July 29. They then waited six weeks before they disclosed the hack to the rest of the population.

This may not be the biggest breach by volume, but it is by far one of the worst we have seen so far in terms of what type of information was stolen. 143 million American's full names, addresses, birth dates, social security numbers and even driver license numbers were exposed during this breach. On top of that, 209,000 people's credit card numbers and 182,000 people's personal dispute details were also exposed. This is a massive amount of data as opposed to other hacks that may have been bigger, but didn't include as much sensitive information. If you have not taken any steps to protect your identity in the past, this should be your turning point. Your information is now out there (if it wasn't before) whether you like it or not and there's not much you can do about it. The other options left are all reactive measures like freezing your credit, monitoring your credit reports and checking your bank statements.

Next Page —>

Equifax Data Breach Continued

Data breaches happen all the time and it was only a matter of time before a major credit bureau would be hacked, but Equifax's poor security protocols are what allowed this breach to happen. A major vulnerability for the backbone of their web server was disclosed, then patched within 24 hours and they failed to apply the patch in a timely manner. Furthermore, an attacker should have been discovered while moving the massive amount of data off of Equifax's server by some sort of security protocol that Equifax had implemented beforehand. Whether that be log files, an IDS/IPS, or some other alert system showing something suspicious was going on at that time, some sort of red flag should have went up much earlier than it did. How often does Equifax move 143 million records off of their servers within a month? Why was all of that data in one place and not compartmentalized to prevent this very thing? And why wasn't all of the sensitive data encrypted?

Equifax waited six weeks to disclose the breach, even then with very limited information on what actually happened. Before they disclosed though, three top level executives just happened to sell shares worth 1.8 million in total. They claim they had no idea until after they sold the shares although the transactions were not part of their scheduled trading plans. Equifax has offered one year of free credit monitoring to all affected consumers. Until recently, signing up would have made you give up your right to sue them. After a lot of backlash, they changed the fine print on the signup form. Equifax is also waiving all fees on credit freezes, allowing everyone (no matter what state you live in) to freeze their credit free of charge. To check the potential impact of this data breach, click on the link below, although it has been proven to be broken and unreliable. It's safe to assume that your data was exposed and you should take steps to protect your information in any way that you can.

https://www.equifaxsecurity2017.com/potential-impact/

EVENTS >>>

Air, Space & Cyber Conference
Sep 18-20 2017, National Harbor, MD

Techcrunch Disrupt
Sep 18-20 2017, San Francisco, CA

Microsoft Ignite
Sep 25-29 2017, Orlando, FL

READER QUESTIONS >>>

Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

Want to **contribute** to the digital update?

Let us know at digitalupdate@tpidg.us

THE EASY BUTTON >>>

Freezing Your Credit

After a huge data breach like the Equifax hack, and before the next hack happens, it's important to take some steps to protect your identity from being stolen (you only have one). One very easy way to do so is by freezing your credit which all three major credit bureaus offer for free or at the most $10 each. With a credit freeze no one, not even you, can take credit out in your name without temporarily lifting the credit freeze with the PIN that you either set or are given by the corresponding credit bureau. You will have the option of temporarily lifting your credit freeze for a certain period of time or letting a predefined organization have access to your credit one time. You will need to do this for each credit bureau that you need to access at that time.

This may seem a bit inconvenient at first, but ask yourself this: when was the last time I needed to take out a line of credit without prior notice? It's not often that a "credit emergency" happens that would prevent you from having the proper amount of time to either unfreeze your credit or write down your pin to unfreeze it on-scene. This should be the default way we have to access our credit anyways, with all of these data breaches your social security number is no longer a secret, your date of birth is everywhere and finding your address is easily done with OSINT. We need some form of extra protection on our credit regardless of whether or not we are at risk of identity theft.

Below are links to freeze your credit with the three major credit bureaus:

TransUnion: https://freeze.transunion.com

Equifax: https://www.freeze.equifax.com

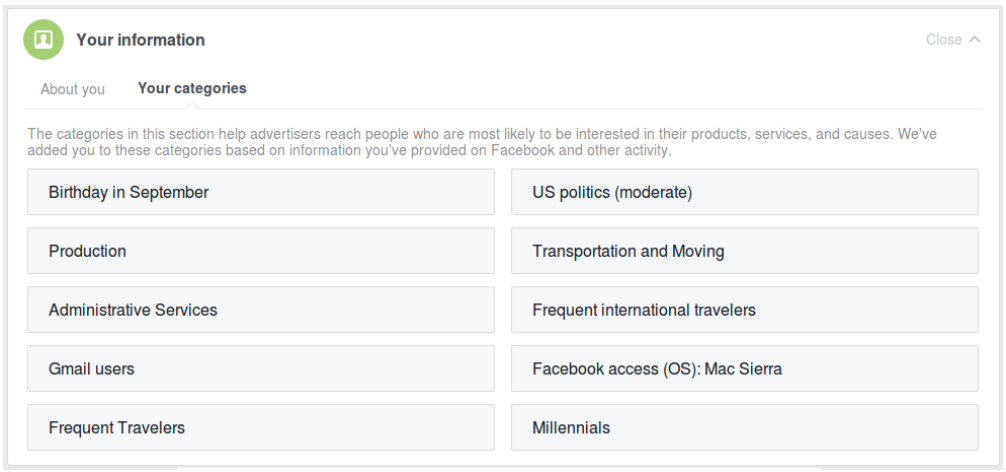
Experian: https://www.experian.com/freeze/

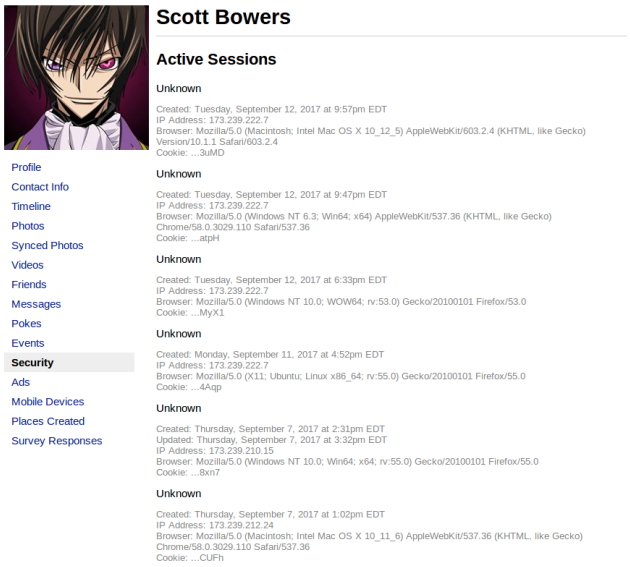
BONUS MATERIALS >>>

Your Facebook Profile

How Facebook Categorizes You

If you ever had any doubts that Facebook has a comprehensive profile of who you are and what you like, head over to https://www.facebook.com/ads/preferences and click on *Your information*, then *Your categories.* This list gives you a pretty good idea of what marketers use to target you when they display ads in your newsfeed. While you're at it, you can download a copy of your data by heading over to https://www.facebook.com/settings and clicking *Download a copy of your Facebook data.* While this is not nearly all of the data Facebook stores on you, it is a massive amount of data. As long as you have a Facebook account, this list of data continues to grow and be added to your existing profile.





UPDATE CORNER >>>

Website Updates

Updates to https://www.tpidg.us for the month of September. For comments or suggestions send an email to admin@tpidg.us

Main Page Changes

- Added a tabbed view of the menu to limit scrolling as more items are added
- Added a data broker opt-out list link under Digital Privacy tab
- Added telemarketer opt-out lists under Digital Privacy tab
- Added a research paper on pattern locks under Forensics tab

Added Car Lookup Tools

- Currently only supports VIN numbers
- Gives full specifications on car

Anything you would like us to add to our website?

Contact admin@tpidg.us

PARTNERS >>>

global communications
arlo
WD
LINKSYS
NETGEAR
FLIR
COMBAT TESTED SINCE 1938 ROTHCO
TOUCHPOINT INTERNATIONAL DEVELOPMENT GROUP, INC
intel Technology Provider
cradlepoint
The World's Sixth Sense
Silent Pocket
Lenovo
DELL
CyberPower Reliability. Quality. Value.
INGRAM MICRO
Technical & Tactical Equipment Store
msi
belkin
Canon
hp
cisco
PPSS
Nitrokey secure your digital life
Honeywell THE POWER OF CONNECTED
redhat
D-Link
vmware
BUFFALO
NVIDIA
KASPER OSWALD Ingenieure für innovative Sicherheitslösungen