TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's New

LAST Chance for a FREE YETI Tundra 105!

See page 2 for more information!

October 2017

This monthly publication provided courtesy of Rick Johnston, President of Information Management Systems

"Enabling People to Provide Great Products and Services - Anytime, Anyplace, Anywhere"

Equifax: Woeful PINs Put Frozen Credit Files At Risk

When is a password not a password?

Never. It's always a password.

No matter what you call it – password, passcode, passphrase, secret, PIN, login or Jeff – and no matter if it is numeric or alphanumeric, under the hood it's the same. The same rules apply on how you choose it and how you store it.

We've been advising the people who have been affected by the giant Equifax data breach to put a freeze on their credit files.

Frozen credit files can't be accessed by creditors, which should stop thieves who stole your identity during the breach from taking out a line of credit in your name. Of course it stops you from taking out credit too but unlike the crooks, you can unfreeze your credit files if you need to. It's far from a perfect solution – freezing and unfreezing isn't slick – but short of changing your SSN and date of birth it's probably your best protection.

What stops the thieves from unfreezing your credit files is a PIN that you know and they don't. Equifax chooses your PIN and gives it to you when you freeze your credit files.

Like all PINs, they're just passwords by another name and the normal rules for choosing passwords apply: the PIN should be long, chosen at random and difficult to guess.

No matter how much a hacker knows about a person or system creating a password, that knowledge shouldn't help. Likewise, knowing a password shouldn't reveal anything about the system that created it or make guessing another one any easier.

That's why we advise that your passwords shouldn't be a child's birthday, a pet's name or your favorite sports team, and why you shouldn't pick passwords according to a sequence or pattern.

In this case, however, you don't get to choose: Equifax does it for you, so the normal rules about choosing passwords apply to them rather than to you.

Not PINs at all

Unfortunately Equifax PINs aren't chosen at random, they are simply the date and time at which you performed your freeze.

If you froze your data on September 8, 2017 at, let's say, 5pm, your PIN would be 0908171700.

The timestamp uses the format MMDDyyHHmm where two characters are used to represent each of: month (01 to 12), day of the month (01 to 31), year, hours since midnight (00 to 23) and minutes (00 to 59).

The PINs are 10 digits long. If Equifax chose numeric PINs at random the crooks would have a one in ten billion chance of guessing the right number on the first go (that still wouldn't count as a strong password by the way, but it's not bad).

By using dates Equifax have slashed the odds on a successful guess.

Even if the system used a randomly-generated timestamp and turned it into a PIN, the system would be flawed.

There are only 365 days in most years, so the MMDD digits don't deliver 10,000 different possibilities (0000 to 9999) as you might expect, and there are only 1440 minutes in a day, which slashes the range of possible values that HHmm can take.

Even if Equifax picked years from anywhere in the last century, the MMDDyyHHmm format would give just 365 × 100 × 1440 variations for a total of just over 50 million different PINs, rather than the 10 billion variations you might reasonably expect the security of the system to be based upon.

Of course, it's much, much worse than that, because Equifax uses the time of your freeze application to lock in your PIN.

> **"If you froze your credit files since the announcement, the odds of guessing your PIN correctly aren't one in ten billion, they're better than one in 5000."**

If you froze your credit files since the announcement, the odds of guessing your PIN correctly aren't one in ten billion, they're better than one in 5000.

If we assume that you didn't freeze your credit files while you were asleep, and that you took at least a few hours to get round to applying for a freeze after hearing the news and deciding what to do, then the odds of guessing the PIN are even better still (better for the crooks, I mean; worse for you).

And that's not the worst of it.

Because of the way the PIN-generating algorithm works, any timestamped logs of your activity on the Equifax systems that are related to your freeze (computers tend to generate a lot of timestamped logs) are effectively *improperly secured copies of your PIN*.

What next?

Unfortunately there is nothing you can do about this, it's all on Equifax. Freezing your credit files remains your best course of action but you should know that the freeze is not as well protected as it should be.

The question is, what will Equifax do next? We think it needs to:

- Acknowledge that its PINs are not fit for purpose and fix them.
- Ensure that PIN entry is "rate limited" to prevent online guessing attacks.
- Promise to tell you if your PIN is hit by a guessing attack.

Please contact us at 701-364-2718 or email info@imsnetworking.com for more information.

This article was written by Mark Stockley—for more information go to: https://nakedsecurity.sophos.com/2017/09/10/equifax-woeful-pins-put-frozen-credit-files-at-risk/

Last Chance for a FREE YETI Tundra!

We love having you as a customer and, quite honestly, wish we had more like you! So instead of just wishing, we've decided to hold a special "refer a friend" event.

Simply refer any company with 10 or more users to our office. We will call and schedule an appointment. When we get the appointment we will send you a YETI Tumbler. If the referral you submitted becomes a client, you will receive a YETI Tundra 105 ($479.99 value!).

To submit a referral please go to: http://www.imsnetworking.com/about-us/referral-program/ or email info@imsnetworking.com

Shiny New Gadget Of The Month:

Picture Keeper Connect, The Best Way To Back Up Photos On The Go

Nothing feels worse than having to delete an old favorite to make room for some new photos. The Picture Keeper Connect solves both of these issues, providing easy-to-use backup for your phone or tablet.

The Picture Keeper Connect, which looks a lot like a conventional flash drive, is designed specifically to back up photos, videos and contact information with just a couple of button presses. It plugs into your phone and gets to work. Even better, it can do all of this without the need for WiFi or network connection. It keeps your photos in their designated album, meaning you won't end up with a cluttered mass of photos when you transfer them to a new device.

Simple, functional, and portable, the Picture Keeper Connect is a must for any avid smartphone photographer.

What is "Dark Web ID" And Why Is It An Absolute MUST To Use In Your Business?

Dark Web ID, is the IT industry's first and ONLY "dark web" monitoring tool that reports in real time when you have been compromised and are actively being sold on the dark web cybercrime underground for the purposes of identity theft or breaches.

Their tool will immediately alert you when your email, passwords, social security number and other personal credentials have been compromised, so you can be on high alert for phishing attacks and identity theft AND direct you to change all of your passwords.

Dark Web ID combines human and sophisticated Dark Web intelligence with search capabilities to identify, analyze and proactively monitor for your organization's compromised or stolen employee and customer data.

Digital credentials such as usernames and passwords connect you and your employees to critical business applications, as well as online services. **Unfortunately, criminals know this—** and that's why digital credentials are among the most valuable assets found on the Dark Web. The Dark Web is made up of digital communities that sit on top of the Internet, and while there are legitimate purposes to the Dark Web, it is estimated that over 50% of all sites on the Dark Web are used for criminal activities, including the disclosure and sale of digital credentials. Far too often, companies that have had their credentials compromised and sold on the Dark Web don't know it until they have been informed

Customers, employees, key executives and high-risk personnel are often targeted and exploited on the Dark Web.

Dark Web ID monitors, aggregates and alerts non-stop—24/7, 365 days a year scouring millions of sources including botnets, criminal chat rooms, peer-to-peer networks, malicious websites and blogs, bulletin boards, illegal black market sites as well as private and public networks and forums.

Save yourself a huge headache and contact us today at 701-364-2718 or info@imsnetworking.com to start providing the best theft monitoring program for your business and employees.

Are Your Digital Credentials For Sale on the Dark Web?

Bits & Bytes

NEVER Throw Your Boarding Pass Away, Not Even After Your Flight

Everybody knows that a boarding pass is mandatory in order to board a plane. While we're in the airport, we keep a close eye on our boarding passes, clutching them in our hands like they're precious gems. But after we land, pretty much everyone ditches the ticket, whether it's lost on the floor, compacted in the washing machine or thrown directly into the trash.

This may seem innocent enough, until you realize the abundance of personal information encrypted on your pass. You'd be amazed at the information a person can glean just by scanning the QR code on the ticket: your home and e-mail addresses, your phone number and even your bank information! When you get rid of your next boarding pass, shred it. Your bank account will thank you.
LuxuryAndGlamor.com 2/5/2016

Are You Missing This One Critical Component In Your Business? If So, You Are GUARANTEED To Be Losing Sales

As Inc. writer Rohit Arora puts it, "It may be 2017, but many companies are still conducting business like it's the 20th century." According to data collected in a recent CNBC report, close to half of small businesses don't even have a website, and even fewer — around 36% — use a website to stay in touch with their customers and prospects. But if we can learn something from Nick's Pizza & Deli in New Jersey, it's that even the smallest companies can leverage new technologies to dramatically increase sales. The restaurant partnered with a company called The Block, a business that builds websites for small businesses, granting them online ordering capabilities. As a result, Nick's owner estimates an increase in annual revenues of around 15% to 20% in only six months. When you make it easy for your customers to pay, you drive further sales. It's that simple. *inc.com 8/6/2017*

You've Been HACKED! What's the First Thing You Should Do?

There's always a chance that IT security will be breached, and one way to make a bad situation worse is not knowing the standard operating procedure when it happens. First, contact your IT personnel. The faster they can address the hack and figure out its extent, the better served you'll be. Next, understand that there are legal ramifications to being hacked; if valuable data has been compromised, you'll have to notify the individuals in question as well as the FBI. Remember, the faster you act, the better it will be.