Krebs on Security

In-depth security news and investigation

- About the Author
- Blog Advertising

18
May 16

As Scope of 2012 Breach Expands, LinkedIn to Again Reset Passwords for Some Users

A 2012 data breach that was thought to have exposed 6.5 million hashed passwords for LinkedIn users instead likely impacted more than 117 million accounts, the company now says. In response, the business networking giant said today that it would once again force a password reset for individual users thought to be impacted in the expanded breach.

The 2012 breach was first exposed when a hacker posted a list of some 6.5 million unique passwords to a popular forum where members volunteer or can be hired to hack complex passwords. Forum members managed to crack some the passwords, and eventually noticed that an inordinate number of the passwords they were able to crack contained some variation of “linkedin” in them.

LinkedIn responded by forcing a password reset on all 6.5 million of the impacted accounts, but it stopped there. But earlier today, reports surfaced about a sales thread on an online cybercrime bazaar in which the seller offered to sell 117 million records stolen in the 2012 breach. In addition, the paid hacked data search engine LeakedSource claims to have a searchable copy of the 117 million record database (this service said it found my LinkedIn email address in the data cache, but it asked me to pay $4.00 for a one-day trial membership in order to view the data; I declined).

Inexplicably, LinkedIn’s response to the most recent breach is to repeat the mistake it made with original breach, by once again forcing a password reset for only a subset of its users.

“Yesterday, we became aware of an additional set of data that had just been released that claims to be email and hashed password combinations of more than 100 million LinkedIn members from that same theft in 2012,” wrote **Cory Scott**, in a post on the company’s blog. “We are taking immediate steps to invalidate the passwords of the accounts impacted, and we will contact those members to reset their passwords. We have no indication that this is as a result of a new security breach.”

LinkedIn spokesman **Hani Durzy** said the company has obtained a copy of the 117 million record database, and that LinkedIn believes it to be real.

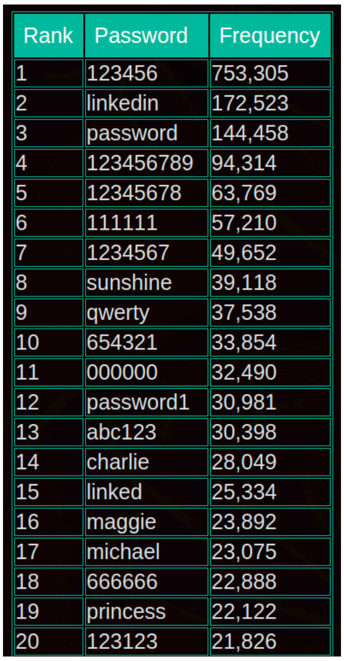
“We believe it is from the 2012 breach,” Durzy said in an email to KrebsOnSecurity. “How many of those 117m are active and current is still being investigated.”

Regarding the decision not to force a password reset across the board back in 2012, Durzy said “We did at the time what we thought was in the best interest of our member base as a whole, trying to balance security for those with passwords that were compromised while not disrupting the LinkedIn experience for those who didn’t appear impacted.”

The 117 million figure makes sense: LinkedIn says it has more than 400 million users, but reports suggest only about 25 percent of those accounts are used monthly.

Alex Holden, co-founder of security consultancy Hold Security, was among the first to discover the original cache of 6.5 million back in 2012 — shortly after it was posted to the password cracking forum **InsidePro**. Holden said the 6.5 million encrypted passwords were all unique, and did not include any passwords that were simple to crack with rudimentary tools or resources [full disclosure: Holden’s site lists this author as an adviser, however I receive no compensation for that role].

“These were just the ones that the guy who posted it couldn’t crack,” Holden said. “I always thought that the hacker simply didn’t post to the forum all of the easy passwords that he could crack himself.”



Rank	Password	Frequency
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652
8	sunshine	39,118
9	qwerty	37,538
10	654321	33,854
11	000000	32,490
12	password1	30,981
13	abc123	30,398
14	charlie	28,049
15	linked	25,334
16	maggie	23,892
17	michael	23,075
18	666666	22,888
19	princess	22,122
20	123123	21,826

The top 20 most commonly used LinkedIn account passwords, according to LeakedSource.

According to LeakedSource, just 50 easily guessed passwords made up more than 2.2 million of the 117 million encrypted passwords exposed in the breach.

“Passwords were stored in SHA1 with no salting,” the password-selling site claims. “This is not what internet standards propose. Only 117m accounts have passwords and we suspect the remaining users registered using FaceBook or some similarity.”

SHA1 is one of several different methods for “hashing” — that is, obfuscating and storing — plain text passwords. Passwords are “hashed” by taking the plain text password and running it against a theoretically one-way mathematical algorithm that turns the user’s password into a string of gibberish numbers and letters that is supposed to be challenging to reverse.

The weakness of this approach is that hashes by themselves are static, meaning that the password “123456,” for example, will always compute to the same password hash. To make matters worse, there are plenty of tools capable of very rapidly mapping these hashes to common dictionary words, names and phrases, which essentially negates the effectiveness of hashing. These days, computer hardware has gotten so cheap that attackers can easily and very cheaply build machines capable of computing tens of millions of possible password hashes per second for each corresponding username or email address.

But by adding a unique element, or “salt,” to each user password, database administrators can massively complicate things for attackers who may have stolen the user database and rely upon automated tools to crack user passwords.

LinkedIn said it added salt to its password hashing function following the 2012 breach. But if you’re a LinkedIn user and haven’t changed your LinkedIn password since 2012, your password may not be protected with the added salting capabilities. At least, that’s my reading of the situation from LinkedIn’s 2012 post about the breach.

If you haven’t changed your LinkedIn password in a while, that would probably be a good idea. Most importantly, if you use your LinkedIn password at other sites, change those passwords to unique passwords. As this breach reminds us, re-using passwords at multiple sites that hold personal and/or financial information about you is a less-than-stellar idea.

Tags: alex holden, Cory Scott, Hold Security, LeakedSource, LinkedIn breach

This entry was posted on Wednesday, May 18th, 2016 at 3:30 pm and is filed under A Little Sunshine, Data Breaches. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.

34 comments

1. *Jonathan Fletcher*
   May 18, 2016 at 4:05 pm

   So THAT’S why they raised their prices and dropped their free option with one week’s notice: because they had such great security! It would only make sense to Kafka.

2. *Jill*
   May 18, 2016 at 4:28 pm

   A reminder that LinkedIn offers 2FA.

   - *Regret*

May 19, 2016 at 12:13 pm

I agree. Another reason why, while imperfect, 2FA helps. Still can't believe some of my financial institutions don't offer it, while social media sites do.

- *Mike*
  May 22, 2016 at 7:41 am

  After the site gets hacked (again), Jill reminds us that 2FA is an option for users. Regret agrees and wonders why more sites don't offer it.

  This is interesting in that it wasn't an individual that got hacked…….It was the site. If 2FA were the answer, this would not even be a topic of discussion. The site is setup for it but it doesn't matter because the site got hacked (again) anyway. Does anyone have the ability to see the forest through the trees?

  - *Matt*
    May 26, 2016 at 10:31 am

    So you leave no room for scenarios where a password db can be stolen and 2FA still provides protection? I can think of at least a few.

    - *Jerome*
      May 26, 2016 at 8:12 pm

      My thoughts exactly! I don't see how this scenario could be an argument for using a single factor, rather than using two factors!

    - *Mike*
      May 26, 2016 at 8:46 pm

      I'm sure there are a few. I'm saying that it's looked at the wrong way. Like so many other things (like https). It's there and it might work or even work well for certain things but you can't apply it universally and expect it to be the be-all-end-all. There are cases (like this one) where it actually becomes a complete waste of time. Like changing your password. When the bad guys already have a level of access that allows them to read your password, that access isn't changed by you changing your password. Whatever you change it to….they still have access to read it. Even if you change it a thousand times. Infact, at that point there is absolutely nothing that any end user can do.

      - *Jerome*
        May 27, 2016 at 5:10 pm

        Nothing is a silver bullet in security, hence the axiom "Defense in Depth"! So the use of 2FA is never a waste of time, it is just another arrow in the quiver so to speak (along with a strong password).

        I don't know where you are going with your statement but passwords are hashed and are not readable no matter the bad guy's access level on a system. If your password is broken due to brute force or a dictionary attack, and if you then change your password, the bad guys no longer have access to your account until they can break your new password (or install a key logger which is easier). Going back to my initial point, even if the bad guys have your username and password, if you are using 2FA they are blocked from accessing your account. So in this instance 2FA saves the day!

        - *Mike*
          May 31, 2016 at 7:18 pm

          lol…..you go on believing all that….

          Meanwhile, I'm reading article after article (some from this site) discussing passwords stored on the servers in plain text and even sometimes right out in the open.

          If LinkedIn were all that, we would not be talking about it. It wouldn't be an issue.

          If 2fa were all that, everyone would be using it and we would be seeing better security all the way around. This is a problem that's getting worse…..NOT better. All it takes is a simple cloud based key-logger coming in from an advertiser that no one wants to filter out. All I'm saying is that people trust this stuff too much.

      - *Jerome*
        May 28, 2016 at 1:02 pm

        Nothing is a silver bullet in security, hence the axiom "Defense in Depth"! So the use of 2FA is never a waste of time, it is just another arrow in the quiver so to speak (along with a strong password).

I don’t know where you are going with your statement but passwords are hashed and are not readable no matter the bad guy’s access level on a system. If your password is broken due to brute force or a dictionary attack, and if you then change your password, the bad guys no longer have access to your account until they can break your new password (or install a key logger which is easier). Going back to my initial point, even if the bad guys have your username and password, if you are using 2FA they are blocked from accessing your account. So in this instance 2FA saves the day!

- *Alex C*
  May 29, 2016 at 8:26 pm

  Disappointingly LinkedIn’s 2FA depends on providing them your phone number. There are many alternative methods for providing 2FA that don’t require submitting your phone number (OAuth, seeded RNGs for phones using various open-source apps, etc.) They’ve shown they can’t be trusted with the data stored in their database so why trust them with yet another piece of your data?

3. *Mike*
   May 18, 2016 at 9:32 pm

   Well they can have it. I have no legitimate use for Linkedin anyway.

   - *Ivan Arnaudov*
     May 19, 2016 at 2:08 am

     Any chance you use the same email/password combination on LinkedIn elsewhere Mike? Because there lies the real trouble – lots of people do, and even if they don’t find value in the services offered by LinkedIn (like you and I), their online safety is compromised by the idiocy of LinkedIn.

4. *Rolf*
   May 18, 2016 at 10:24 pm

   LinkedIn looked like a good idea when it first started but it quickly became a pain in my arse. Within a few weeks of signing up I was being email-bombed with invitations from hundreds of strangers and it took 10 months and dozens of emails to escape from their death grip. It is easier to opt out of Facebook than LinkedIn.

   - *rod*
     May 19, 2016 at 3:44 am

     I opted out 6-7 years ago and the buggers still pester me.

   - *Moike*
     May 19, 2016 at 7:32 am

     I never signed up, but was conscripted by a web scraper who scraped the web site where I worked. I was listed on LinkedIn at the position listed in the company web site on an unclaimed profile.

     I still get LinkedIn derived spam directed at me in that old position, long since left.

   - *treFunny*
     May 19, 2016 at 9:40 am

     yeah its trash … just like facebook, twitter, etc.

5. *Alan Ralph*
   May 19, 2016 at 3:35 am

   Worth mentioning that some other sites allow you to login using your LinkedIn credentials, so the potential reach for hackers or malcontents goes a lot further than LinkedIn’s website.

   I changed my password as soon as I found out in 2012, and now have 2FA enabled on all the services I use that support it. Incidents like this, and the Adobe hack that occurred in 2013, remind me that I have to take control of my online security, since I cannot be certain that all services I use have a grip on this.

   - *Robert.Walter*
     May 19, 2016 at 11:57 am

     Your 2nd para are words to the wise but might be improved with the realization that a seeming minority of websites have security under control and in some card as we’ve seen the biggest of operations have done a callously poor job (exceedingly poor if corrected for size and resources) of protecting their users.

6. *Robert.Walter*
   [May 19, 2016 at 5:19 am]

   Here linked in will looks 6 times bad, all pretty much due to their own missteps:
   1. Vulnerable system
   2. Weak hashing
   3. No salting
   4. Assuming partial breech
   5. Partial resets
   6. (2016) more partial resets

   If they had their proactive organizational skills and crisis management wits about them, they should have been able to prevent 5 of these (I assume no system is in vulnerable, and stood hacker with luck can enter even the top tier systems.)

   The take-away as I see it for others is:
   1. Harden your system
   2. Harden your data at rest
   3. If breach occurs, assume it's a full one, even if you have no evidence to support such an extreme conclusion
   4. Announce that it may be a breach of limited extent, but from an abundance of caution all passwords are being reset.
   5. Have good rules in place that:
   a. Block the most common passwords (and variants with related character strings)
   b. Set required parameters (15 digit, low and hi letters, numbers and symbols) and show these in the p/w setup panel
   c. Offer 2FA
   d. Require a mobile phone number or alternate email address for backup recovery
   e. Along with (d.) explain the benefits of not using an employer mobile number (i.e. if you have your own mobile number: if your employer drops mobile, or you leave company, you may not be able to recover a lost p/w), and the benefits of using a non-employer-/non-ISP-provided, non-obscure-ISP email address for recovery (i.e. privacy, policy-change resistant, portability, penetration risk). Preferred solution private mobile number and big email provider email account).
   f. Configure your system to support and not frustrate u/n and p/w a user's p/w-manager's autofill attempt.

7. *Fernando Ardenghi*
   [May 20, 2016 at 5:58 am]

   And eHarmony's?
   And PlentyOfFish (POF)?
   and other online dating sites like Match, OkCupid?

   Soon?

8. *Hayton*
   [May 21, 2016 at 7:11 pm]

   LinkedIn didn't ask me to reset my password at the time of the first reports of a breach, but I thought, it's only a tiny percentage of their user base so I won't bother.

   This time the percentage of their user base is much, much bigger but they still haven't suggested I reset my password. All the same, after reading this I reset the password on LinkedIn and now I have to look for any other sites where that password was also used and change those too (yes, I know. But there are only so many unique passwords I can remember).

   Given that LinkedIn is no longer as useful as it once was (just my personal opinion) it might be best to live without it – although others have said that LinkedIn invites and notifications can continue even after you unsubscribe.

   - *JohnO*
     [May 27, 2016 at 8:44 am]

     Don't remember them, use a password manager to generate truly random passwords and store them for you. Then you only need to remember 2, one for your phone and one for the password manager.

9. *Bill*
   [May 25, 2016 at 1:34 am]

   haveibeenpwned.com now shows my LinkedIn account as certainly compromised (meaning: it's public data now)… but still not a peep from LinkedIn recommending that I reset my password…

   @Brian, I think they are just pulling your leg that they've asked "some" users to reset their passwords… I dunno which "some" they might be referring to… a couple company execs maybe? Obviously not little people like me.

   - *BrianKrebs*
     [May 26, 2016 at 1:03 pm]

     Well, I got the message today, as did a number of people yesterday judging from my inbox of forwarded emails from readers who received the same.

Notice of Data Breach
You may have heard reports recently about a security issue involving LinkedIn. We would like to make sure you have the facts about what happened, what information was involved, and the steps we are taking to help protect you.
What Happened?
On May 17, 2016, we became aware that data stolen from LinkedIn in 2012 was being made available online. This was not a new security breach or hack. We took immediate steps to invalidate the passwords of all LinkedIn accounts that we believed might be at risk. These were accounts created prior to the 2012 breach that had not reset their passwords since that breach.
What Information Was Involved?
Member email addresses, hashed passwords, and LinkedIn member IDs (an internal identifier LinkedIn assigns to each member profile) from 2012.
What We Are Doing
We invalidated passwords of all LinkedIn accounts created prior to the 2012 breach that had not reset their passwords since that breach. In addition, we are using automated tools to attempt to identify and block any suspicious activity that might occur on LinkedIn accounts. We are also actively engaging with law enforcement authorities.
LinkedIn has taken significant steps to strengthen account security since 2012. For example, we now use salted hashes to store passwords and enable additional account security by offering our members the option to use two-step verification.
What You Can Do
We have several dedicated teams working diligently to ensure that the information members entrust to LinkedIn remains secure. While we do all we can, we always suggest that our members visit our Safety Center to learn about enabling two-step verification, and implementing strong passwords in order to keep their accounts as safe as possible. We recommend that you regularly change your LinkedIn password and if you use the same or similar passwords on other online services, we recommend you set new passwords on those accounts as well.
For More Information
If you have any questions, please feel free to contact our Trust & Safety team at tns-help@linkedin.com. To learn more visit our official blog.

- *Mike*
  May 27, 2016 at 7:55 pm

  Truthfully, the whole thing sounds more like they are just cleaning house and getting rid of old data. What better way of expediting the process?

  - *Jerome*
    May 28, 2016 at 1:19 am

    I can think of many different, and better ways, to get rid of data which doesn't open yourself to lawsuits and drag your corporate name through the mud

    - *Mike*
      May 28, 2016 at 5:40 am

      What? Like Enron? Like these kinds of things don't happen? Companies are made of people and those people don't always do what makes sense. From the top CEO down to the janitor. It happens. Companies are destroyed all the time by stupid stuff. We are told constantly about companies being dragged through the mud due to things the company itself set into motion. Some of it ends up for discussion on this site.

    - *Mike*
      May 28, 2016 at 6:06 am

      FBI raids dental software researcher who discovered private patient data on public server

      http://www.dailydot.com/politics/justin-shafer-fbi-raid/

      Tell me that there is no potential for lawsuit here. Tell me that there were better ways of handling this.

- *Alex C*
  May 29, 2016 at 8:22 pm

  I just got the same message, too, but the offer of two-step verification requires users to give LinkedIn their phone numbers (presumably to receive a text message with a login code) instead of using some other authentication method like OAuth or the various one-time-password applications around for phones and computers. If they couldn't be trusted with passwords, why would anyone provide their phone number, too?

- *CJ*
  June 9, 2016 at 6:17 pm

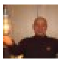
  I received my notice on May 27
  Notice of Data Breach

10. *Jerome*
    May 27, 2016 at 5:24 pm

The Top 20 LinkedIn passwords is shocking! Any dictionary attack would find these trivial to break, and this is after all of the news articles about the consequences of weak passwords and any work related security training they have received!

11. Annie Bai
June 1, 2016 at 12:08 pm

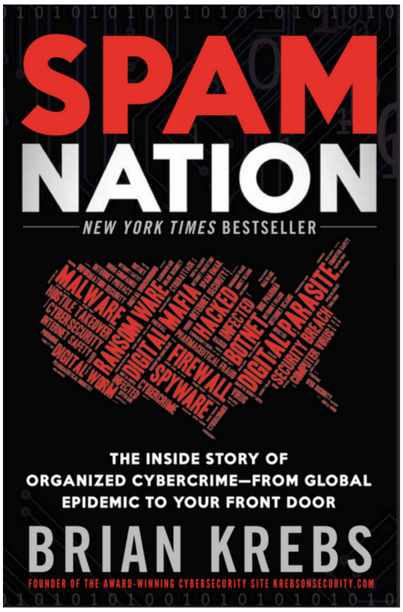
I have a related question, Brian. How can we find out what kind of data LinkedIn accesses on a device?
1. Apps – In my iPhone privacy settings, I do not see that LinkedIn has requested access to my Contacts, Calendars, Location, or other.
2. Granular Data – And what about other data, such as battery usage and all that other "creepy" stuff?
Thanks!

12.  Joe
June 16, 2016 at 8:17 am

We need to embrace the reality that Encryption can be broken – period!
Until this myth is dispelled, we won't move past it to a more security data security.

-

- ## My New Book!


SPAM
NATION
NEW YORK TIMES BESTSELLER
THE INSIDE STORY OF ORGANIZED CYBERCRIME—FROM GLOBAL EPIDEMIC TO YOUR FRONT DOOR
BRIAN KREBS
FOUNDER OF THE AWARD-WINNING CYBERSECURITY SITE KREBSONSECURITY.COM

A New York Times Bestseller!

- Buy at Amazon
- Donate with PayPal

- ## Recent Posts

  - Trump's Dumps: 'Making Dumps Great Again'
  - MolinaHealthcare.com Exposed Patient Records
  - Should SaaS Companies Publish Customers Lists?
  - Private Eye Allegedly Used Leaky Goverment Tool in Bid to Find Tax Data on Trump
  - Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division

-

- ## Subscribe by email

Please use your primary mailbox address, not a forwarded address.

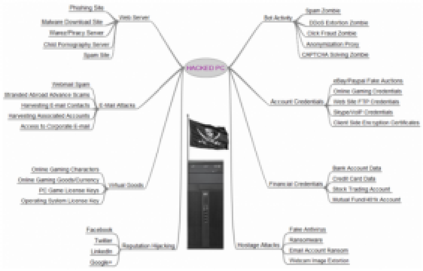
Your email:
Enter email address...

Subscribe Unsubscribe

- ## All About Skimmers

Click image for my skimmer series.

- ## The Value of a Hacked PC



Badguy uses for your PC

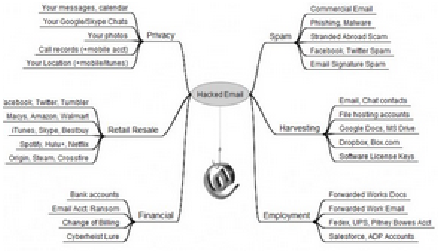
- ## Tools for a Safer PC

Tools for a Safer PC

- ## The Pharma Wars

Spammers Duke it Out

- ## Badguy Uses for Your Email



Your email account may be worth far more than you imagine.

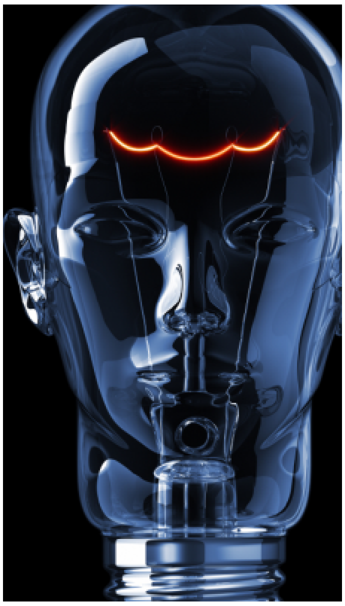
- ## eBanking Best Practices

eBanking Best Practices for Businesses

- ## Most Popular Posts

  - Online Cheating Site AshleyMadison Hacked (798)
  - Sources: Target Investigating Data Breach (620)
  - Cards Stolen in Target Breach Flood Underground Markets (445)
  - Reports: Liberty Reserve Founder Arrested, Site Shuttered (416)
  - Was the Ashley Madison Database Leaked? (376)
  - True Goodbye: 'Using TrueCrypt Is Not Secure' (363)
  - Who Hacked Ashley Madison? (360)
  - Following the Money, ePassporte Edition (353)
  - U.S. Government Seizes LibertyReserve.com (315)
  - Extortionists Target Ashley Madison Users (310)

- ## Category: Web Fraud 2.0

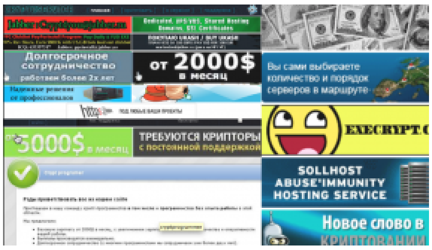


Innovations from the Underground

-

  ID Protection Services Examined

- ### Is Antivirus Dead?

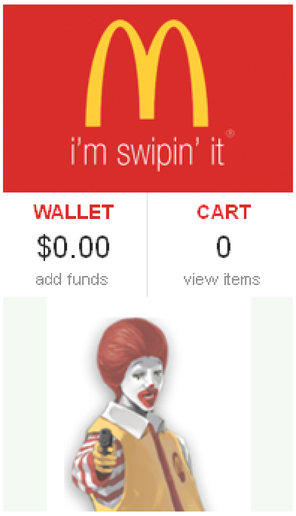
  
Долгосрочное сотрудничество
работаем более 2х лет
от 2000$ в месяц
Вы сами выбираете количество и порядок серверов в маршруте
EXECRYPT
5000$ в месяц
ТРЕБУЮТСЯ КРИПТОРЫ с постоянной поддержкой
SOLLHOST ABUSE-IMMUNITY HOSTING SERVICE
Новое слово в криптовании

  The reasons for its decline

- ### The Growing Tax Fraud Menace

  File 'em Before the Bad Guys Can

- ### Inside a Carding Shop

  A crash course in carding.

- ### Beware Social Security Fraud

my Social Security– Sign In Or Create An Account

At each stage of your life, my Social Security is for you. Your personal online my Social Security account is a valuable source of information beginning in your working years and continuing throughout the time you receive Social Security benefits.

If you receive benefits or have Medicare, you can:

Use a my Social Security online account to:

- Get your benefit verification letter;
- Check your benefit and payment information and your earnings record;
- Change your address and phone number; and
- Start or change direct deposit of your benefit payment.

Sign up, or Be Signed Up!

- ## How Was Your Card Stolen?

Finding out is not so easy.

- ## Krebs’s 3 Rules…

...For Online Safety.

Powered by WordPress. Privacy Policy