**AFM News and Views**

**February 2020**

****

210 W. Jackson St. - Morton, IL 61550
Phone: (309)266-5400 - Fax: (309)266-5400

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

***Our mission*** *is to serve our clients, in an atmosphere of trust, to help grow and preserve their wealth.  We provide personal attention and comprehensive strategies, striving to enable our clients to live and retire with stability. Alltrust Financial Management serves clients seeking comprehensive financial guidance, with a team approach, in a manner that continuously exceeds our clients' expectations. We are a recognized and respected financial management firm delivering trusted, personal attention.*

**Boys and girls have an equal aptitude for math — so why are there are so few women in higher paying STEM jobs?
Source:www.marketwatch.com**

**Women make up just 26% of people in computer and mathematical occupations, according to the BLS**

New research suggests that the gender gap in so-called STEM careers — science, technology, engineering and mathematics — may be more due to nurture than to nature.

A study published in the peer-reviewed journal “[Science of Learning](https://www.nature.com/articles/s41539-019-0057-x)” found that the brains of young boys and girls react the same to mathematics problems, and yet women make up 26% of people in computer and mathematical occupations, 21% of computer programmers and 16% of those in architecture and engineering, according to the Bureau of Labor Statistics.

Researchers found that boys and girls aged between 3 and 8 performed the same on mathematical tests, and magnetic resonance imaging of their brains age 3 to 10 “showed significant gender similarities in neural functioning” while watching mathematics education videos, the researchers add.

“Across multiple neural analyses, we show that girls’ and boys’ brains function similarly during mathematical processing,” write authors Jessica Cantlon, the Ronald J. and Mary Ann Zdrojkowski professor of developmental neuroscience and associate professor of psychology at Carnegie Mellon University, Alyssa Kersey, postdoctoral scholar at the University of Chicago’s Department of Psychology, and Kelsey Csumitta at University of Rochester’s Department of Brain and Cognitive Science in Rochester, N.Y.

The brains of 104 children age 3 to 10 were scanned using functional MRI while watching mathematics education videos. “We saw no evidence of gender differences in neural responses to mathematics content, neural responses during educational video viewing, or rates of neural development for mathematical processing in early childhood, and in fact we found statistical equivalence between boys and girls throughout the brain,” the researchers write.

The research was combined with other statistical data on how young boys and girls performed on certain mathematical tests, they added.

The paper helps address the vexed issue of why STEM professions remain heavily skewed toward men. The authors say the belief remains widespread that women are naturally less good at STEM subjects. “Some have suggested that girls and women are under-represented in careers in STEM owing to biological differences,” they note.

In 2017, Google   fired software engineer James Damore for raising “biological causes” between men and women[as one possible explanation for the company’s heavy employment bias toward men](https://www.marketwatch.com/story/this-is-the-real-reason-why-women-are-underrepresented-in-science-and-tech-2017-08-09). In 2005, Harvard University professor Larry Summers provoked a furor [with similar remarks](https://www.theguardian.com/science/2005/jan/18/educationsgendergap.genderissues), and the incident was seen as a key factor in his resignation the following year.

“How many more studies do we need to show that boys and girls bring the same cognitive skills to learning across all disciplines?” asks Carroll Serron, professor emerita of criminology, law and society at University of California, Irvine and an author of [research](https://journals.sagepub.com/doi/10.1177/0730888415618728) on gender and careers. “As our work makes clear, the challenge is to address the cultural barriers that women and under-represented minorities face in the STEM fields; this will require that those in positions of power come to terms with their stereotypes and biases — a tall order to be sure.”

[Other research](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933241) has shown that by the time they reach middle and high school, boys on average out perform girls in math — and that outperformance is the top reason boys are more likely to pursue STEM careers.

Meanwhile, STEM careers are among the most lucrative. Graduates in STEM-related fields were expected to earn the highest average starting salaries among eight broad job categories, according to a 2019 salary survey by the National Association of Colleges and Employers. A 2019 graduate with a bachelor’s degree in engineering was projected to make an average starting annual salary of $69,188; a computer science graduate was expected to earn an average of $67,539 per year; a math and sciences grad was expected to make $62,177 per year.

That compares to an average annual salary of $56,651 for a humanities major, $57,657 for a business major and $57,310 for a social sciences major.

One possible barrier for women entering STEM fields: An unwelcoming work environment that can sometimes include discrimination. Women working in STEM jobs are more likely to say they have experienced discrimination in the workplace (50% versus 41% in other fields), [a 2018 Pew Research Center survey](https://www.pewsocialtrends.org/2018/01/09/women-and-men-in-stem-often-at-odds-over-workplace-equity/) found. In STEM jobs, “discrimination and sexual harassment are seen as more frequent, and gender is perceived as more of an impediment than an advantage to career success,” Pew found.

The latest paper adds to the growing literature showing the relative importance of nurture over nature in the gender disparities, says Lina Anaya Beltran, co-author of [research](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068971) on the subject. For example there are [multiple](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2008733) [studies](https://cgeg.sipa.columbia.edu/sites/default/files/cgeg/WP53-3Eble.pdf) showing the influence of environment on whether girls are likely to perform well at math.

“This is study is very interesting, because they are looking at the brains of young children,” she says. Beltran says more research needs to be done. But she added, “The more I read about this topic, the more I believe nurture plays a bigger role.”

**5 ways to keep your money safe from hackers in 2020**

Source:www.marketwatch.com

If 2019 taught us anything, it was that it’s just a matter of time before hackers find our personal information online.

After a string of major hacks affecting millions of internet users, there are few people left online who haven’t been affected. With 100 million Capital One  customers [having their sensitive data exposed](https://www.marketwatch.com/story/the-capital-one-data-breach-exposes-a-new-dark-side-to-credit-card-rewards-2019-07-30) on top of last year’s Equifax breach   exposing [the data of 148 million customers](https://www.marketwatch.com/story/equifax-breach-was-entirely-preventable-congressional-report-says-2018-12-10), Marriott   exposing [500 million users’ information](https://www.marketwatch.com/story/after-massive-hack-marriott-pledges-to-pay-for-new-passports-if-fraud-has-taken-place-2018-12-03), and Exactis exposing [the data of more than 340 million people](https://www.marketwatch.com/story/what-is-exactisand-how-could-it-have-the-data-of-nearly-every-american-2018-06-28), your information is at a higher risk than ever.

Here are five easy steps you can take to make yourself — and your finances — less hackable.

**Use a password manager**

Too many people still use passwords like “123456” and “password” to keep their accounts secure, [according to a report from software company SplashData](https://www.marketwatch.com/story/your-password-probably-sucks%E2%80%94%E2%80%94heres-how-to-make-it-stronger-2018-05-04) on the ‘100 Worst Passwords of the Year.’ Passwords that are that easy to guess put you at risk — and it isn’t hard to do better. Using a password manager will keep all of your accounts secure with unique and complex passwords, and you only have to remember one: [the password master](https://www.marketwatch.com/story/the-last-password-youll-ever-need-to-remember-2018-04-30).

To do this, set up an account at a well-known manager service like Lastpass, 1Password, Dashlane, Keeper, or Password Boss. While there is a negligible risk the password manager itself could be hacked, experts say any manager is still safer than trying to remember your own passwords.

**Turn on two-factor authentication**

Make sure to turn on two-factor authentication on your password manager as well as for accessing individual websites. This security feature verifies your identity before you log on to a site by sending a code to your phone through text message or email. The website Turn It On: The Ultimate Guide to Two-Factor Authentication, allows users to search for any site they are logging into to see if it offers the feature. Besides text verification, there are other two-factor options, including a Yubikey, a $45 USB device that you can plug into a computer to verify that you are the correct user.

**Change your router password**

After several high-profile breaches involving internet routers, it would be wise to [change the default password on any device](https://www.marketwatch.com/story/why-you-should-change-your-internet-router-password-now-2018-11-13)in your home that’s connected to the internet. Often when you purchase an internet router, it comes with a default string of letters and numbers as the password. These passwords [areeasily available on online forums](https://www.marketwatch.com/story/why-you-should-change-your-internet-router-password-now-2018-11-13), on the dark web and the regular internet, making it possible for hackers to get into your home network and every device connected to it. Changing your home network password is one of the most simple ways to avoid getting hacked.

 **Change your default DNS**

An easy way to strengthen your online security in just a few clicks is to [change the default Domain Name System (DNS)](https://www.marketwatch.com/story/this-30-second-change-to-your-computer-settings-is-the-easiest-way-to-stop-hackers-2018-06-12) used by your internet service provider to a safer alternative. Changing the address to Google, 8.8.8.8, or Cloudflare 1.1.1.1, or Quad9, 9.9.9.9 offers better protections against hacking. This can be done through ”Control Panel” on a Windows device or “System Preferences” on a Mac device.

**Freeze or lock your credit**

A 2018 federal law [made it free](https://www.marketwatch.com/story/freezing-your-credit-is-now-free-2018-09-21) for consumers to freeze their credit at all three major credit bureaus: Equifax, Experian   and TransUnion. Meanwhile, the three bureaus have made freezing or locking one’s credit report much easier by introducing mobile apps that allow consumers to block or un-block access to their credit information on the go.

Given [how common it is](https://www.marketwatch.com/story/why-you-should-freeze-your-credit-even-if-you-werent-involved-in-the-marriott-breach-2018-11-30) for companies to get hacked these days, this is a simple step that can prevent hackers from stealing a consumer’s information and using it to open fraudulent credit accounts.

***monthLY contest***

*2020 is the Year of the vision. So, this year, we are going to do some eye trivia.* We will pick a random winner each month among the correct answers we receive.

**This Month’s Question**: What is the biggest part of the eye?

Please email your responses to alltrust@lpl.com

***results of last month’s contest***

**Question :** What do you call the colored part of your eye?

*Answer: Iris*

Last month’s winner: Jean Turney

***Weekly updates are available***

LPL Financial’s ***Weekly Market Commentary*** and ***Weekly Economic Commentary*** can be found on LPL Financial’s website (<http://www.lplfinancial.com/learning_center/research/>).

***Other updates available from LPL Research department***

* Daily market update: <http://LPLresearch.com>
* YouTube Channel: <http://www.youtube.com/lplresearch> (which can also be found on our website)

***CLIENT CONNECT***

Are you anticipating an e-mail change? Let us know. We want to make sure you receive all of our e-mail communications. Send your new e-mail to melissa.arbisi@lpl.com

If you have any input or comments about our newsletter, let us know. We love to hear from you!!

Your referrals mean a great deal to our business. If you know of a friend or family member who might benefit from our service, please let us know. We will work hard to ensure that your referrals feel it was a wise investment of their time – and their future- to have met with us.

Don’t keep us a secret!! Share this with your family and friends.

Till next month,

The Alltrust Team

Securities offered through LPL Financial.  Member FINRA/SIPC

The opinions voiced in this material are for general information only and are not intended to provide specific advice or recommendations for any individual. To determine which investment(s) may be appropriate for you, consult your financial advisor prior to investing.

The information is being provided for general educational purposes only and is not intended to provide legal or tax advice. You should consult your own legal or tax advisor for guidance on regulatory compliance matters. Any examples provided are for informational purposes only and are not intended to be reflective of actual results and are not indicative of any particular client situation. Stock investing involves risk including loss of principal.