

Risk, reward, and economic value - for the Digital Age.



January Letter

Hi **First name**,

OK, I'm a tad tardy for 2019's first monthly newsletter. Here's why.

TDS spent the holiday break and most of January adding improvements and security features to our services. Private Email accounts and Device Protection have both received upgrades that meaningfully increase their security and performance for the customer.

More on the new security enhancements below. But January also kept us busy with these new cases:

- \$2 million in personal funds - home computer and email hack.
- \$156,000 lost by a small-business due to an employee using a personal (un-secure) email account for company business.
- Over \$500,000 lost by an individual investor using an AOL account.
- \$1.5 million business loss from an email hack.
- \$200,000 loss as a result of a hacked internet-connected fish-tank sensor.
- And several other cases with losses ranging from a few hundred dollars, to over \$50,000.

The common denominator

The cybersecurity industry reports over 85% of successful hacks start with an email account.

Our data says over 90% of hacks come from email.

So, want to eliminate most of your risk in one swoop that is easy and affordable?

Create a **Private Email** account that gets you off the grid of risk and abuse by hackers and Big Tech. [Click](#) to get a complimentary consultation and estimate.

You will never regret the decision. And you will do it eventually. So be preemptive, especially where it matters so much.

Privatizing email gets you away from AOL, Yahoo, Gmail, MSN, Hotmail, the baby-bells (the \$156,000 loss reported above started on a bellsouth.net email account.) And it will work to protect for the rest of your life as you shift banking, investment, professional advisors, and others to your secure email account.

We make privatizing your email easy and affordable and suggest adding boxes for family members too.

A hacked fish-tank?

Have you heard the term "Internet of Things?"

I'm always surprised there will be somewhere between **25 to 50 billion** of them by 2021.

These "things" are smart, aware, and connected devices and appliances like Ring doorbells, IP security cameras, smart TV's, and increasingly all that surrounds us - even fish-tanks.

These internet-connected "things" are each an on-ramp to your network. They each provide an inbound lane to your computers, personal information, and the surveillance of all your online activities.

Every time a new "thing" is connected to the internet, it expands the cybercriminal's attack surface and provides them with a barn-door open to your stuff - like the \$200,000 loss stemming from the living room fish-tank reported above.

What to do about managing these "things" and taking control of your information? Secure your router, home and office networks, and Wi-Fi. It's called Router Network Security and [here's how it works](#).

New security enhancements for customers

The holiday break 2018 / 2019 at TDS was spent adding new layers of protection for our customers and the services we provide.

- We did it behind the scenes, with no outage or interruption for our customers.
- We charged no additional costs or fees.

At TDS, continually incorporating the latest innovation and science from the IT security industry is core to our mission:

"Make best-in-class, enterprise-grade IT security solutions accessible, affordable, and easy to use for people on their personal technology."

Here is a snap-shot of what we did to increase security for our customers:

- **Private Email Accounts** - Added **DKIM** - DomainKeys Identified Mail - an email authentication method that stops spam, phishing, and spoofing. Read more about DKIM and how it works in the top tile below.
- **Device Protection** - Added significant performance improvements to our F-Secure Device Protection engine - the service that secures your Mac, Windows, and Android devices 24/7/365. In real-time, no less.
 - Database size reduced by over 50%
 - Network bandwidth reduced by 50%
 - Faster auto-updates with no restarts required - pretty amazing.
 - New machine learning and advanced software systems reduce false-positives by well over 25%.

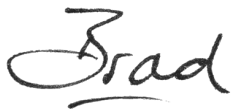
What this all means is simply this; greater security and less in your way - just the way we like it.

Finally, I'm really happy the [MIT Technology Review](#) has invited and added me to their **Global Review** board.

Founded in 1899, the magazine is wholly owned by the Massachusetts Institute of Technology, but editorially independent of the university.

I have lots to say, a ton of field-borne experience to share, and so much I want to learn from others that will be participating in the Review for 2019.

Thanks for reading,

A handwritten signature in black ink that reads "Brad". The signature is written in a cursive, slightly stylized font with a horizontal line under the name.

February 2, 2019