The CyberAdvisor Newsletter

February 2020

Hi There,

Do you ever think about what is going to happen over the next five or ten years as a couple of generations find their lives are like the proverbial fly in the amber - recorded and preserved for all history to see?

It's easy to understand how bad that can go but really hard to reason with and influence those that don't know or care. We see plenty of that at TDS and think this article from the MIT Technology Review is spot on when they say:

> **"it's not just individuals who might suffer. Something much larger—the potential for social change and transformation—may also be at risk."**

The fly in the amber images are a visual expression of what our kids need to know and understand. New, digital age life-skills are required for survival and success in the future, and in the U.S., we aren't being led to change.

PETER CROWTHER

Every day we help families adapt and impress upon their kids the value of privacy, personal information, and digital autonomy. Contact us if we can help you and yours.

Damage Tolls

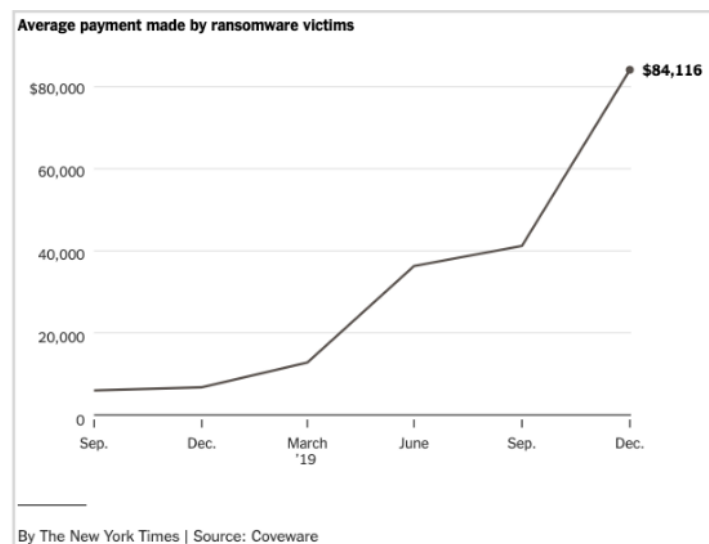The FBI just released its annual record on cybercrime for 2019. The New York Times reports on the facts:

The New York Times Feb. 9, 2020

Ransomware Attacks Grow

Hackers are locking people out of their networks and demanding big payments to get back in. New data shows just how common and damaging the attacks have become.

Here are some of the report's key points:

- $3.5 billion in total damages, up 350% since 2015.
- The FBI's run-rate for new reports is 1,200 per day.
- Victims aged 60+ represented almost $1 billion of the damages.

Most astounding is the average ransom cost, up almost 1,000 percent in a little over a year.

Average payment made by ransomware victims

$84,116

$80,000

60,000

40,000

20,000

0

Sep.   Dec.   March '19   June   Sep.   Dec.

By The New York Times | Source: Coveware

In 2015 I wrote about ransomware, the evolution of extortion, and that cybercrime was going mainstream. When you couple cyber with any crime, it makes the act far easier and safer to perpetrate than its traditional form.

The loot is digital currency, which for bad guys means anonymity, portability, and liquidity - the perfect treasure chest. The pool of potential victims is limitless and for the most part, oblivious, unarmed, and faceless.

It's not surprising we are seeing cybercrime grow at rates dwarfing anything humanity has seen.

> "... ransomware has evolved into an industry, with hundreds of gangs vying for the most lucrative victims. Some hackers have specialized in "ransomware as a service" ... they have even built out customer-service centers to deal with victims and their payments."
>
> "Anything of value that is smart and connected can be compromised and held for ransom,"
>
> "The F.B.I. noted in its latest warning that the attacks were becoming "more targeted, sophisticated, and costly."
>
> The New York Times

The full report by the FBI is here, and the NY Times article here.

By the way, cryptocurrency scams took in more than $4b in 2019. Read more from the Wall St. Journal, here.

Macs Now More Vulnerable Than PCs

Did you know, for the first time Macs are now more vulnerable to malware than PCs.

> "Malware targeting Apple's Mac devices is growing at a faster rate than ever before, a new report by Malwarebytes is suggesting. As a matter of fact, it has grown so widespread that it managed to outpace PC malware this year for the first time."
>
> IT Pro Portal, February 12th, 2020

See the top news tile below for more about Mac malware, understanding adware, and the trends at hand.

Wi-Fi Hacking

New variants of ransomware now target networks and potential victims from the area <u>around them</u>. It's like getting a disease from someone across the street, without ever having encountered them or the infection before.

Emotet Malware Now Hacks Nearby Wi-Fi Networks to Infect New Victims

📅 February 12, 2020   👤 Ravie Lakshmanan   **The Hacker News**

"Emotet, the notorious trojan behind a number of botnet-driven spam campaigns and ransomware attacks, has found a new attack vector: using already infected devices to identify new victims that are connected to nearby Wi-Fi networks." The Hacker News, Feb.12 2020

Adding insult to injury for Wi-Fi, this from Phillips on February 5th:

Flaw in Philips Smart Light Bulbs Exposes Your WiFi Network to Hackers

The Dark Side of Smart Homes

In the latest research shared with The Hacker News, Check Point experts today revealed a new high-severity vulnerability affecting Philips Hue Smart Light Bulbs that can be exploited over-the-air from over 100 meters away to gain entry into a targeted WiFi network.   February 5th, 2020.

*** Ransomware attacks on home and office Wi-Fi's will soar over the next several years. Good passwords are essential and Managed Network Security provides comprehensive and autonomous security 24/7. More, here.

How Private is Your Email?

From a cyber risk standpoint, bad things typically start with an email. Easily, it's nine times out of ten where the victim's email account is the "vector" for an attack's successful penetration.

Like Auckland, NZ's mayor, Phill Goff, many do not understand the vulnerability and risks they take when using common email services.

Phil Goff's emails hacked - 15,000 emails over 12 years offered for sale

8 Feb, 2020 5:00am   The New Zealand Herald   ⏱ 6 minutes to read

"Emails apparently sent and received by Auckland mayor Phil Goff over a 12-year period have been offered with a $20,000 price tag and appear to contain deeply personal information alongside council and Parliamentary work."

"Like thousands of other account holders across the country he assumed the service provider's email platform was secure. While the authenticity of the hack has not been verified, the Mayor has discontinued use of the email account and taken advice from experts."

One of the smartest things one can do for survival and success in the digital age is to privatize their personal email accounts. And in our experience, nothing works better than a family email domain to get family members onboard.

To see an example of email gone bad in a really big way, [check out](#) the victims fund where every Yahoo Mail account at the time of the breach was hacked.

We're Growing!

TDS is growing and in 2020 we added two important partnerships to our business.

- **Private Clients** - A nationally recognized wealth management company added TDS as a preferred provider. The firm serves wealthy individuals, entrepreneurs, professionals, athletes, and family offices with financial planning and investment management services. We're excited to be able to work with their trusted advisors to provide our privacy and digital security solutions to their clients and their families.

- **Executive Services** - The CEO of a large NYSE company became a customer in January after an extensive period of due diligence by his firm in 2019. Now, we're working with the company to add senior executives and corporate board members to protect their homes and personal computers with the same enterprise cybersecurity [solutions](#) we provide to all our clients.

While this new business is "institutional," I assure you, our delivery is still very much "personal." The most effective approach to cybersecurity combines enterprise-grade protection with an individual that is aware, informed, and can think critically when confronted with things not seen before.

Buying a New Computer?

Over the past couple of years, we've had clients ask us for help buying their next computer. We help them determine which brand and model is the most suitable and represents the best value for their needs.

We assist in the order process, take delivery on their behalf, and outfit it with Computer Protection, Private Email, and a VPN. Then we ship it, and the client receives their new computer locked down with all security functions installed and ready to go.

We aren't charging clients for the service during February and March, so contact Diane if you're thinking about a new computer.

Thanks for reading,

Brad

Brad Deflin

Macs Outpace Windows for Malware

Macs are more vulnerable to malware than PCs for the first time. IT Pro Portal, Feb.12, 2020.

Read More

- -

Wealthy people like the Amazon chief Jeff Bezos are often a persistent target of hackers.   David Ryder/Getty Images

Phone Hacks Can Happen to Anyone. Here's How to Protect Yourself.

Start by knowing what could expose you to an attack, like vacation clues, hotel Wi-Fi and inadequate verification procedures. NY Times, Jan. 31, 2020.

Read More

How to Take Control of Your Notifications

Apps and websites regularly push alerts to your devices, but there are ways to minimize disruption and still stay in the loop. NY Times, Feb 5, 2020.

Read More

11 Simple Tips to Effective Email Management

At the end of the day, email is just a tool for you to get your tasks done. Here are 11 tips to improve your email management. LifeHack, Feb. 2020.

Read More

99 Updates for Windows in February

And Adobe issues dozens more. Software updates are critical for privacy and security. The Hacker News, Feb. 11, 2020.

Computer Protection from TDS does the updating for you, quickly and automatically as soon as updates are released.

Read More

The Best Way to Start Protecting Today? Privatize Your Personal Email

Go private! Well over 80% of cybercrime originates with an email.

- Own your email - not Big Tech.
- Professionals, families - for privacy, security, and physical safety.
- Your digital safe-zone for life.

Start