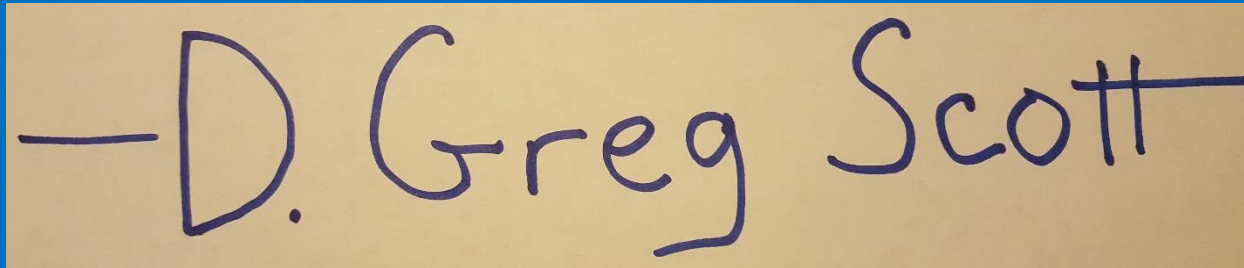


# Cybersecurity

**What** We're up Against and **How** to Kick Bad  
Guys' Butts



—D. Greg Scott—

CISSP Number 358671



Who says IT is boring?

# Boring statistics that hit home


From <https://www.broadbandsearch.net/blog/alarming-cybercrime-statistics>

- A cyberattack happens once every 39 seconds.
  - “The computers in our study were attacked, on average, 2,244 times a day.”
- 78 percent of organizations in the US experienced a cyberattack in 2019.
- 23 percent of Americans have either had their credit card or financial information stolen by attackers, or they know someone who has.
- Data breaches effected 30 percent of all US consumers in 2018.
- The U.S. economy loses between \$57 billion and \$109 billion per year to malicious cyber activity.

# Eight seconds in my basement

- Oct 7 12:38:55 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=171.242.158.152 DST=216.160.2.135 LEN=44 TOS=0x00 PREC=0x00 TTL=49 ID=60708 PROTO=TCP SPT=34494 DPT=23 WINDOW=47045 RES=0x00 SYN URGP=0
- Oct 7 12:38:59 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=195.54.161.104 DST=216.160.2.136 LEN=44 TOS=0x00 PREC=0x00 TTL=241 ID=39863 PROTO=TCP SPT=42098 DPT=218 WINDOW=1024 RES=0x00 SYN URGP=0
- Oct 7 12:39:00 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=192.241.220.248 DST=216.160.2.133 LEN=44 TOS=0x00 PREC=0x00 TTL=246 ID=54321 PROTO=TCP SPT=40013 DPT=110 WINDOW=65535 RES=0x00 SYN URGP=0
- Oct 7 12:39:00 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=171.235.221.124 DST=216.160.2.136 LEN=52 TOS=0x00 PREC=0x00 TTL=49 ID=29656 DF PROTO=TCP SPT=50326 DPT=445 WINDOW=8192 RES=0x00 SYN URGP=0
- Oct 7 12:39:02 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=79.66.18.65 DST=216.160.2.133 LEN=40 TOS=0x00 PREC=0x00 TTL=53 ID=0 DF PROTO=TCP SPT=54355 DPT=443 WINDOW=0 RES=0x00 RST URGP=0
- Oct 7 12:39:03 infra2020-fw kernel: IN=enp2s0 OUT= MAC=00:30:18:c5:e3:b8:a0:a3:e2:63:de:20:08:00 SRC=45.234.63.120 DST=216.160.2.132 LEN=52 TOS=0x00 PREC=0x00 TTL=115 ID=16530 DF PROTO=TCP SPT=54750 DPT=445 WINDOW=8192 RES=0x00 SYN URGP=0



A man with brown hair, wearing a yellow Star Trek uniform with a black collar and a Starfleet insignia on the chest, is crouching in a desert landscape. He is smiling and looking towards the camera. The background shows a rocky, arid environment with some sparse vegetation. A blue speech bubble is positioned to the right of the man, containing the text "I need more than statistics and numbers. Give me real stories."

I need more than  
statistics and  
numbers. Give me  
real stories.



[Home](#) > [Security](#) > [Data Breach](#)

OPINION

# OPM's \$63 million breach settlement offer: Is it enough?

The nature and scope of the data stolen in the U.S. Office of Personnel Management presents a life-long risk to victims, who might get as little as \$700 if the court accepts the settlement.

By **Christopher Burgess**

CSO | JUN 2, 2022 2:00 AM PDT

DELL  
Technologies

DELL PRECISION 3560  
MORE SUSTAINABLE  
FOR A BRIGHTER FUTURE  
[Learn More >](#)

Intel® Core™ i7  
processor

Metamorworks / Getty Images

DELL  
Technologies

PRECISION 3560



# Supply Chain Attack: The Big One in 2020

solarwinds



*The Power to Manage IT*

# What's a Supply Chain Attack?



Spy movie – good guys planning how to save the world.

Image from <https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/>



# What's a Supply Chain Attack?



But the good-guy room is bugged. Bad guys are listening.

Image from <https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/>

Q: How would bad guys plant bugs in every good-guy room in the world?



Image from <https://www.deadgoodbooks.co.uk/nicholas-searle-realistic-spy-movies/>

# A: Take over the lightbulb factory



Plant bugs in every lightbulb.

When good guys change bulbs, bad guys own another room.



But I'm not big enough for anyone to attack



LOCAL

# Prison for Minnesota man who posed as federal agent

His defense attorney said Reyel Simmons did not benefit financially but "was merely playing dress-up to impress people around him and to woo women."

By Paul Walsh (<https://www.startribune.com/paul-walsh/6134706/>) Star Tribune |

JUNE 8, 2022 — 11:46AM

A southern Minnesota man has been sentenced to six years in prison for posing as a Department of Homeland Security officer on social media, where he built a following of thousands and lured unsuspecting women into relationships.

Reyel D. Simmons, 53, of Dodge Center, Minn., was sentenced in U.S. District Court in St. Paul last week after pleading guilty in January to impersonating a federal officer and illegal weapons possession. Simmons' sentence includes three years of supervision after he leaves prison.

Before sentencing, prosecutors argued for Judge Eric Tostrud to give Simmons a term of more than seven years, pointing out that he carried out his scheme behind his wife's back while at the same time dating the woman who eventually turned him in.

Defense attorney James Becker proposed a two-year sentence. Becker noted that Simmons had an alcoholic mother and was raised in Denver by alcoholic grandparents. He also struggled with dyslexia and attention-deficit disorder in school.

Becker acknowledged in a court filing that his client "maintained his fictional biography with several women with whom he had romantic relationships, including the woman he married and deceived for many years."

But, the attorney continued, he "never accrued any financial benefit ... and never sought to use his (mis)identity to gain access to restricted areas or information. ... In truth, Mr. Simmons was merely playing dress-up to impress people around him and to woo women."

According to court documents:



FEDERAL COURT RECORDS

Reyel Simmons made a habit of posing as a federal law enforcement agent or a member of the military.

FBI looking for more victims of


https://www.kare11.com/article/news/local/breaking-the-news/fbi-looking-for-more-victims-of-st-paul-sextortio

KARE 11 News Weather Near Me VERIFY Watch Live

ADVERTISE WITH US KARE 11+ LOCKED ON SPORTS MINNESOTA LINKS KARE 11 INVESTIGATES BREAKING THE NEWS

## FBI believes there are more victims of St. Paul man's sextortion scheme

More than 500 minors have already been identified as victims, but agents say they believe there may be more.



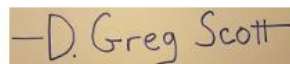
Author: Sharon Yoo  
Published: 6:07 PM CDT June 15, 2022  
Updated: 6:59 PM CDT June 15, 2022

BROOKLYN CENTER, Minn. — A St. Paul man has pleaded guilty to a massive sextortion

August Sage  
ARTISAN HANDCRAFTED HOME GOODS  
SHOP NOW

- FBI Supervisory Special Agent Brenda Born says Chu Vang targeted 500 minors.
- "We were able to uncover approximately 75 identifications and monikers he was using to communicate with the victims," Born said.





# We Kidnapped your Fiancé. Pay up or She Dies.

by Greg Scott | Mar 22, 2022 | Cybersecurity | 0 comments



A person who lives near me originally posted this story on Facebook about how somebody claimed to have kidnapped his fiancé. I am sharing it here with his permission. He posted the story on Wednesday, March 16, 2022. This is his story in his own words. I edited for grammar and spelling, cleaned up a few sentences, and rearranged a couple paragraphs for clarity. I also used fictional names. With the benefit of hindsight and years of cybersecurity experience, I'll share some thoughts after his story.

This happened to me on Monday. I'm writing this as warning to everyone of the evil that's out there. Don't be taken onto a rollercoaster like I was.

I left work to go pick up my daughter and come back to work as I do on my days with my kiddos. On the road, I received a phone call from a local number. I answered to woman on the other line very hysterical and in panic, crying. A man took the phone and told me my girlfriend had been in a car accident and that she was uncontrollable. I heard the cries from this woman and I could swear it was my fiancé. He told me she had been in a bad car accident and I needed to come there. He asked me to talk to her and calm her down. He put her back on the phone and I could hear her cries. I told her its okay baby, its all going to be okay, as my heart dropped and couldn't figure out exactly what was going on.

 Search

## Follow Us



## Recent Posts

Fake email notification  
phishing

Copyright Phishing

2nd Amendment Phishing  
Scam

The Day a Hard Drive Crash  
Almost Killed General Motors

We Kidnapped your Fiancé.  
Pay up or She Dies.

## Recent Comments

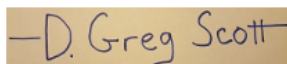
Elizabeth on When a Madman  
Controls the Checks and  
Balances

Toni Braton on When a  
Madman Controls the Checks  
and Balances

Greg Scott on Death Threat  
via Twitter Phishing Scam

Toni Post on Death Threat via  
Twitter Phishing Scam

Ken on Hollywood Hackers –  
Guess the Password. Save the



## Fake email notification phishing

by Greg Scott | Jun 6, 2022 | Phish collection

I see at least one fake email notification from my email administrator every day. Which is hilarious because I am my email administrator. They usually claim I exceeded a quota or have some other problem. Most have English grammar problems. But this one –...

## Copyright Phishing

by Greg Scott | May 24, 2022 | Phish collection

This is a pretty good scam against anyone operating a website. I'll give this one a B+. Your website violates my copyright. Click here to find out what you violated. If you don't fix it, I'll sue you for \$zillions. It knocks me off balance and makes...

## 2nd Amendment Phishing Scam

by Greg Scott | May 16, 2022 | Phish collection

This phishing scam to lure American 2nd Amendment activists could have been a classic. It starts nicely, referencing a telephone call I was never on to throw me off balance. And then they plagiarize NRA outrage statements that flew around Twitter months ago to really...

## Seriously? Your account requires advanced security from Facebook Protect

by Greg Scott | Mar 9, 2022 | Phish collection

Want to know the real insult with this email? It's legitimate. I checked the email header and it really did come from Facebook. The "Turn on Facebook Protect" button really does go to Facebook. That's right. Facebook sent me this notice and it...

 Search

### Follow Us



### Recent Posts

Fake email notification phishing

Copyright Phishing

2nd Amendment Phishing Scam

The Day a Hard Drive Crash Almost Killed General Motors

We Kidnapped your Fiancé. Pay up or She Dies.

### Recent Comments

Elizabeth on When a Madman Controls the Checks and Balances

Toni Braton on When a Madman Controls the Checks and Balances

Greg Scott on Death Threat via Twitter Phishing Scam

Toni Post on Death Threat via Twitter Phishing Scam

Ken on Hollywood Hackers – Guess the Password, Save the

# Here's where it gets personal



# I am a repeat cyber victim myself.

- Late November, 2011, somebody tried to steal more than \$14,000 with one of my credit cards
  - I tracked down names, dates, and details and gave it all to the FBI
  - We traded a few emails and then.....
  - I'm still waiting
- 2008 Norm Coleman for Senate Campaign
  - Details here:  
<http://www.dgregscott.com/gross-security-lapse-hurt-us-senate-campaign/>
- November, 2000 attack against my DNS server
- The FBI and I go way back.  
<https://www.dgregscott.com/the-fbi-and-bureaucracy-and-me/>



# How?



**How** do bad guys plunder good guys, seemingly at will?

And **why** do business leaders and politicians keep hiding behind weenie excuses?

Browser window showing the website **DeepDotWeb** (https://www.deepdotweb.com/about-deepdotweb/).

**Navigation Bar:**

- BREAKING NEWS: DARKNET VENDORS AND BUYERS SWITCHING TO DECENTRALIZED TRADING SOLUTIONS
- ADVERTISE ON DEEPPOTWEB
- WRITE FOR US
- ABOUT DEEPPOTWEB
- OUR PGP KEY
- DDW ONION SITE

**Header:**

- DEE.DOT.WEB  
Official Hidden service:  
DeepDot35Wvmeyd5.onion
- Bitcoin Casinos: BEST BITCOINS CASINOS, Free 200% Signup Bonuses, PLAY NOW

**Menu:** HOME, NEWS & ARTICLES, MARKETS LIST, MARKETS CHART, VPN'S CHART, BITCOIN CASINOS, BTC MIXER, Q&A ~ ASK HERE!, VIDEOS, CONTACT US, SEARCH...

**Breadcrumbs:** HOME » ABOUT DEEPPOTWEB

**Warning:** WARNING ISP'S ARE LOGGING YOUR TOR USAGE [Read More >>](#)

**Social Media:**

- RSS: SUBSCRIBE TO RSS FEED
- Twitter: 7,051 FOLLOWERS
- Facebook: 2,566 FANS

**Subscription:** SUBSCRIBE FOR NEW POSTS NOTIFICATIONS: YOUR EMAIL HERE [SUBSCRIBE ME!](#)

**ABOUT DEEPPOTWEB**

This page provides a short introduction and insight about DeepDotWeb.

Some of you may already know a lot about our website, but most of you probably don't. Here are some things you should know about DeepDotWeb:

- We are a team that gathers information and educates the public on everything related to the dark net.
- Not all of us are native English speakers, so we apologize for any spelling or grammatical errors in our posts and articles.
- This site is a hobby of ours, our main business lies in internet assets.
- We established DeepDotWeb in the wake of our friend being arrested by local authorities, for buying drugs from the original Silk Road marketplace. Our aim is make information about dark net markets accessible to everyone, as well as making the dark net safer by reporting on security risks, scams and operations conducted by law enforcement. By providing

**MUST READ:**

- Updated List of Dark Net Markets
- [Click Here To Buy Bitcoins With Paypal!](#)
- Dark Net Markets Comparison Chart
- Best VPN service Comparison Chart
- How To Buy Drugs Online?
- Jolly Roger's Security Guide for Beginners
- MultiSig Guides
- Security Tutorials

**Advertisements:**

- SLOTS: BITCOIN CASINO REVIEWS up to 200% Deposit Bonuses PLAY NOW!
- MIX YOUR COINS - BE SMART, STAY ANONYMOUS
- Warning!!! Your Tor Usage Is Being Watched

How do  
bad guys  
win?

They  
collaborate.



DeepOnionWeb | Deep Web Ne X

https://www.deeponionweb.com

deep onion web

Markets & Shops Onions Tutorials Contact Us

### Onion List & Availability Status

#### TOR Directory

Onion.Live [Copy URL](#)

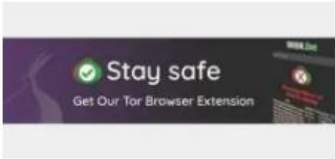
#### Darknet Markets

White House Market	<a href="#">Show URLs</a>
Versus Market	<a href="#">Show URLs</a>
Big Blue Market	<a href="#">Show URLs</a>
Empire Market	<a href="#">Show URLs</a>
Dream Market	<a href="#">Show URLs</a>
The Majestic Garden	<a href="#">Show URLs</a>
Cannazon Market	<a href="#">Show URLs</a>
Cannahome Market	<a href="#">Show URLs</a>
Dark Market	<a href="#">Show URLs</a>
Yellow Brick Market	<a href="#">Show URLs</a>
Hydra Market (RU)	<a href="#">Show URLs</a>
Tor Market (NZ)	<a href="#">Show URLs</a>

#### Scam Markets


### DEEPPONIONWEB.COM

**Important Note:** We do not use referral links or receive payments from any darkweb market.




[MARKETS](#) / [VENDOR SHOPS](#) / [FORUM](#) / [FRAUD](#) / [GUIDES](#) / [NEWS](#)

#### Onion.Live Tor Browser Extension




[VENDOR SHOPS](#)

#### Hanf4You




[MARKETS](#)

#### Cannahome Market




[FORUM](#)

#### Deutschland



[FRAUD](#)

#### flugsvamp



[GUIDES](#)

#### Torum

### Must Read

[Onion.Live Tor Browser Extension](#)

[Is the Tor network really that safe?](#)

[Easy ways to buy crypto-currencies worldwide](#)

[Multisig vs Escrow vs Finalize Early, and what they mean.](#)

["What PGP is" and how to use it in a few easy steps.](#)

### Categories

- [Top Markets](#)
- [Markets](#)
- [Vendor Shops](#)
- [Forum](#)
- [Fraud](#)
- [Guides](#)

And they adapt

CA:Symantec Issues - MozillaW X +

https://wiki.mozilla.org/CA:Symantec\_Issues

Log in Request account

[[  ]]

mozilla wiki

Main page  
Product releases  
New pages  
Recent changes  
Recent uploads  
Random page  
Help

How to Contribute  
All-hands meeting  
Other meetings  
Contribute to Mozilla  
Mozilla Reps  
Community Portal

MozillaWiki  
About  
Team  
Policies  
Report a wiki bug

Around Mozilla  
Mozilla Support  
Mozilla Developer Network  
Planet Mozilla  
Mozilla Blog  
Research

Tools  
What links here  
Related changes  
Special pages  
Printable version  
Permanent link  
Page information  
Import an Etherpad  
Browse properties

Page Discussion

Read View source View history Search

## CA:Symantec Issues

Following the investigation documented below, a [consensus proposal](#) was reached among multiple browser makers for a graduated distrust of Symantec roots. The dates in that proposal and how they apply to Mozilla's Root Program and Firefox are as follows:

- December 1st, 2017: Symantec to implement "Managed CA" proposal
- January 2018 (Firefox 58): Notices in the Developer Console will warn about Symantec certificates issued before 2016-06-01, to encourage site owners to migrate their TLS certs.
- May 2018 (Firefox 60): Websites will show an untrusted connection error if they have a TLS cert issued before 2016-06-01 that chains up to a Symantec root.
- October 2018 (Firefox 63): Removal/distrust of Symantec roots, with caveats described below.

Note: Mozilla's planned release content and schedules are subject to change.

This page lists all confirmed issues involving the CA "Symantec". It may be further updated by Mozilla as more information becomes available. Please do not edit this page yourself; if you have proposed changes, email [Wayne](#). Information here is correct to the best of Mozilla's knowledge and belief. Symantec has also [confirmed](#) the accuracy of the information, although errors transcribing their statements into this page remain Mozilla's.

The issues are in broadly chronological order by end date.

Contents [hide]

- Issue B: Issuance of 1024-bit Certificate Expiring After Deadline (Dec 2013 - Jan 2014)
  - Symantec Response
  - Further Comments and Conclusion
- Issue C: Unauthorized EV Issuance by RAs (January 2014 - February 2015)
  - Symantec Response
  - Further Comments and Conclusion
- Issue D: Test Certificate Misissuance (April 2009 - September 2015)
  - Symantec Response
  - Further Comments and Conclusion
- Issue E: Domain Validation Vulnerability (October 2015)
  - Symantec Response
  - Further Comments and Conclusion
- Issue F: Symantec Audit Issues 2015 (December 2014 - November 2015)
  - Symantec Response

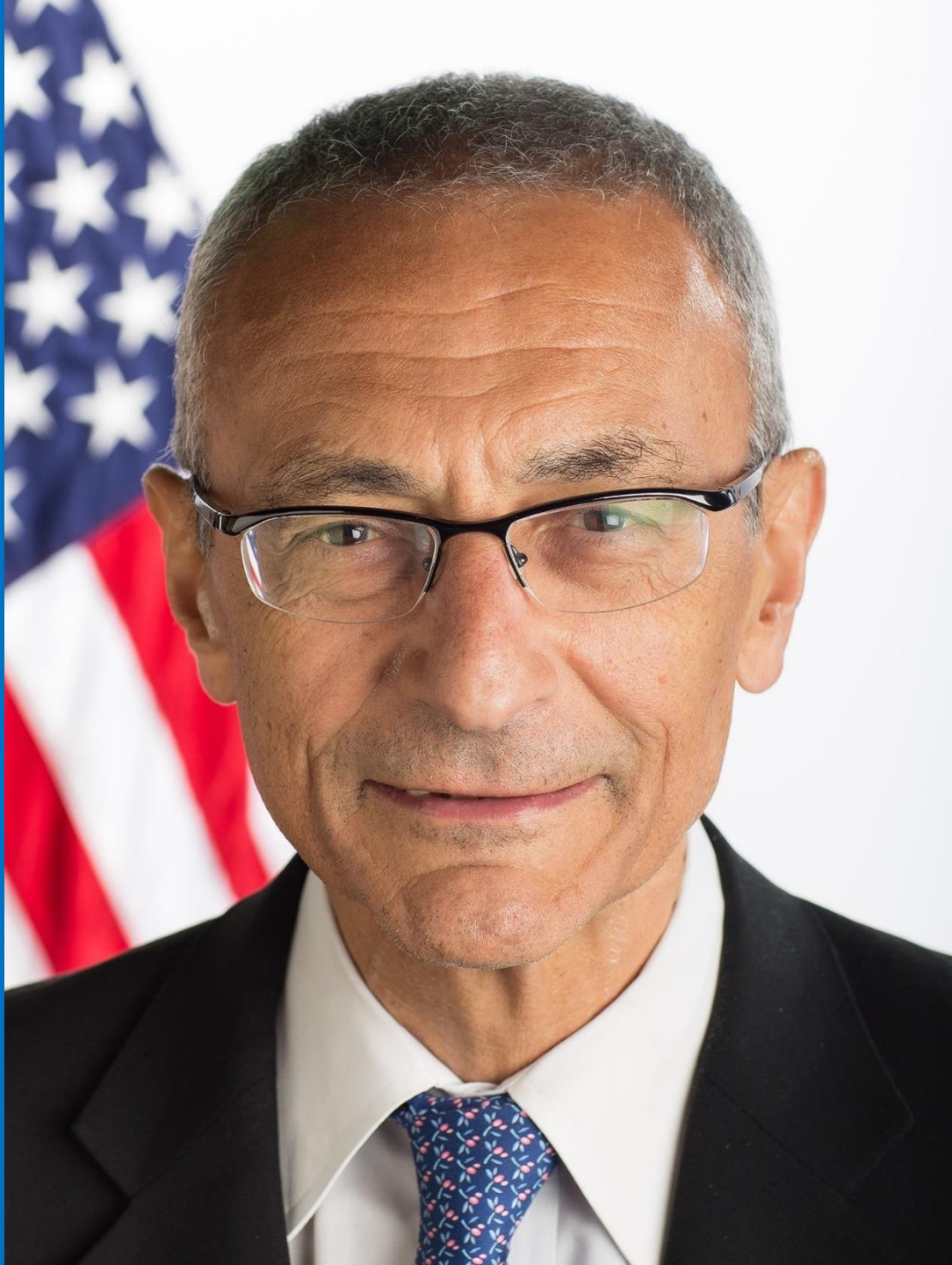
How do  
good guys  
lose?

CA trust  
failures



Institutional failures





## Willful ignorance

- John Podesta, Hilary Clinton campaign manager.
- He gave his email password to the Russians in a 2016 phishing scam.



Willful ignorance on both sides of the political aisle

- Norm Coleman, former US Senator from Minnesota.
- Exposed a spreadsheet with private donor information on his campaign website in 2008.





Stolen government attack  
tactics

# Asleep at the Switch

solarwinds



*The Power to Manage IT*







# Time to recap – what are we up against?

- Bad guys have a vast underground supply chain and support network.
- The entities we're supposed to trust with the Internet security infrastructure have all been compromised.
- Personal information about nearly all adult Americans is up for sale on underground websites.
- Thousands of businesses have been compromised.
- The United States government is both a perpetrator and a victim.
- If your identity is stolen, law enforcement is unwilling or unable to help.
- Lies fly around the planet lots faster than truth.



Maybe we should  
just give up

Buy a cave in Montana and hide.

Pay with cash.

Bad guys have unlimited time and creativity.

You don't!

Does giving up make you mad? It should.






Because we need to win



# A Winning Strategy - Layers of Defense

- 
- Email Hygiene
  - Patching
  - Authentication
  - Trust
  - Passwords
  - Backups
  - Social Media
  - Mobility
  - Tech Tools
  - Awareness
  - Six words to summarize everything
  - Two great books

# Social Media and Disinformation Campaigns



<https://www.computerweekly.com/opinion/Its-time-to-accept-that-disinformation-is-a-cyber-security-issue>



The Twilight Zone, Season 1, Episode 22: The Monsters are Due on Maple Street,  
March 4, 1960









# The firehose of falsehood





# Versus

See <https://www.rand.org/pubs/perspectives/PE198.html>



# The squirt gun of truth





# MIT: Lies travel farther and faster than truth

- See <https://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308>
- “We found that falsehood diffuses significantly farther, faster, deeper, and more broadly than the truth, in all categories of information, and in many cases by an order of magnitude,”
- False news stories are 70 percent more likely to be retweeted than true stories.
- It takes true stories about six times as long to reach 1,500 people as it does for false stories to reach the same number of people.
- When it comes to Twitter’s “cascades,” or unbroken retweet chains, falsehoods reach a cascade depth of 10 about 20 times faster than facts.
- Falsehoods are retweeted by unique users more broadly than true statements at every depth of cascade.



# 2019 social media mob up close and personal

- See <https://www.dgregscott.com/when-dakota-county-mn-charged-my-11-year-old-grandson-with-5th-degree-assault-for-playing-in-a-park-in-a-costume/>



# Comet, COVID, Conspiracies, Chaos



SOURCE: SNIPS FROM PLANDEMIC VIDEO  
YOUTUBE AND FACEBOOK



See

<https://www.dgregscott.com/information-warfare-is-a-cybersecurity-thing-duh/>



December 27, 2020 at 12:02 PM · 🌐



**Donald J. Trump** ✓

December 26, 2020 at 9:50 AM · 🌐

The "Justice" Department and the FBI have done nothing about the 2020 Presidential Election Voter Fraud, the biggest SCAM in our nation's history, despite overwhelming evidence. They should be ashamed. History will remember. Never give up. See everyone in D.C. on January 6th.



Election officials follow strict rules and have found no evidence of widespread fraud.

Source: Bipartisan Policy Center

[Get Accurate Election Info](#)



5 Comments



Like



Comment



Share



**Greg Scott**

I'd challenge President Trump to present one piece of evidence that stands up to scrutiny.

Like · Reply · 3w



**Greg Scott** wow 🤔 what news channel are you watching???? They have the servers from Germany with every bit of blatant evidence, you did not know that?

Like · Reply · 3w





January 6, 2021





# The Russians do it too



# What do we do about it?

## Social media companies

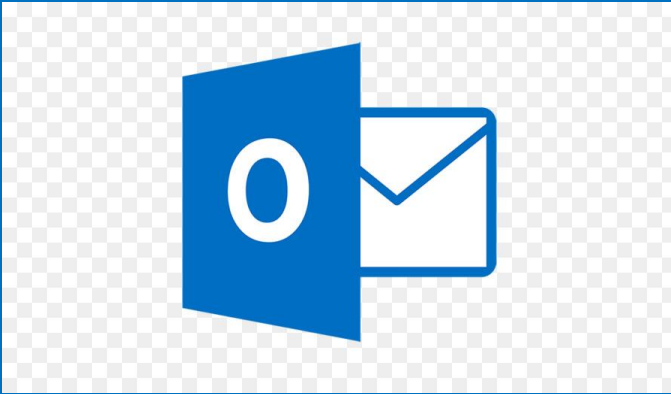
- Ad-hoc censorship was a knee-jerk reaction and self-defeating.
- Adopt circuit breakers, similar to stock market circuit breakers.
- Amplify opposing points of view.
- But business models built on maximizing emotional engagement.

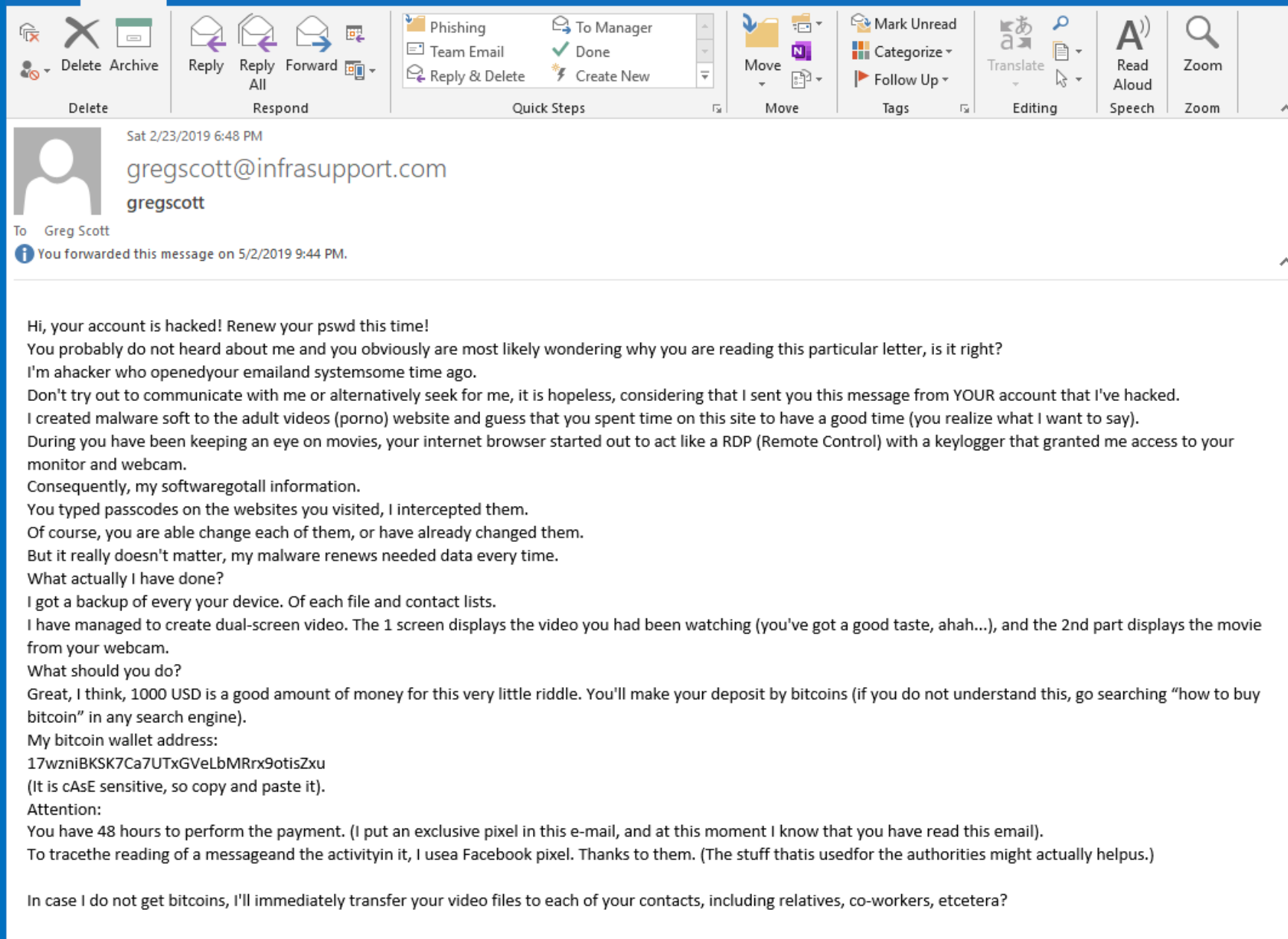
## The public

- Learn to understand how social media companies make money.
- Think before sharing.
- Seek out opposing points of view.



# Email hygiene





For lots of phishing samples, see <https://www.dgregscott.com/category/phishy-emails/>

# Patching





# Authentication





# Trust



See <https://www.dgregscott.com/internet-trust-mini-seminar/>



# Passwords/Passphrases





# Which do you like better?

A complex password with random characters: jHdfgy&4Jq\*7

Or

A good passphrase: goodpassphrasesbeatcomplexpasswords

Goodpassphr@ses

See

<https://www.dgregscott.com/passwords-must-die-long-live-passphrases/>

# Backups





# Mobility





# Tech Tools

```
root@infra2009-fw:~
May  7 04:01:52 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=113.68.190.243 DST=216.160.2.133 LEN=44 TOS=0x00 PREC=0x00 TTL=52 ID=54327 PROTO=TCP SPT=50897 DPT=23 WINDOW=43697 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:01:56 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=206.189.181.12 DST=216.160.2.129 LEN=44 TOS=0x00 PREC=0x00 TTL=57 ID=11438 PROTO=TCP SPT=34377 DPT=23 WINDOW=37977 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:04 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=01:00:5e:00:00:01:a0:a3:e2:63:de:20:08:00 SRC=192.168.0.1 DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2 MARK=0x1
May  7 04:02:04 localhost kernel: IN=br0 OUT=br0 PHYSIN=eth0 PHYSOUT=eth1 SRC=192.168.0.1 DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2 MARK=0x1
May  7 04:02:12 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=209.17.97.82 DST=216.160.2.134 LEN=44 TOS=0x08 PREC=0x20 TTL=247 ID=54321 PROTO=TCP SPT=49562 DPT=9000 WINDOW=65535 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:17 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=5.253.86.126 DST=216.160.2.133 LEN=44 TOS=0x00 PREC=0x00 TTL=247 ID=59200 PROTO=TCP SPT=53985 DPT=445 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:23 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=188.64.129.121 DST=216.160.2.129 LEN=52 TOS=0x08 PREC=0x20 TTL=112 ID=16846 DF PROTO=TCP SPT=52072 DPT=445 WINDOW=8192 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:25 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=103.91.9.20 DST=216.160.2.132 LEN=44 TOS=0x00 PREC=0x00 TTL=247 ID=27630 PROTO=TCP SPT=15727 DPT=23 WINDOW=0 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:30 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=103.91.9.20 DST=216.160.2.133 LEN=44 TOS=0x00 PREC=0x00 TTL=247 ID=23433 PROTO=TCP SPT=44186 DPT=23 WINDOW=0 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:33 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=198.108.67.63 DST=216.160.2.136 LEN=44 TOS=0x00 PREC=0x00 TTL=40 ID=45409 PROTO=TCP SPT=41469 DPT=3098 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:37 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=187.84.147.165 DST=216.160.2.129 LEN=44 TOS=0x00 PREC=0x00 TTL=241 ID=11861 DF PROTO=TCP SPT=57349 DPT=81 WINDOW=14600 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:45 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=34.195.46.204 DST=216.160.2.129 LEN=40 TOS=0x00 PREC=0x00 TTL=243 ID=51168 DF PROTO=TCP SPT=443 DPT=53526 WINDOW=0 RES=0x00 RST URGP=0 MARK=0x1
May  7 04:02:45 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=81.22.45.219 DST=216.160.2.133 LEN=44 TOS=0x08 PREC=0x20 TTL=239 ID=10481 PROTO=TCP SPT=47374 DPT=61000 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:47 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=185.176.26.101 DST=216.160.2.136 LEN=44 TOS=0x00 PREC=0x00 TTL=242 ID=8619 PROTO=TCP SPT=45040 DPT=16581 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:51 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=172.217.4.234 DST=216.160.2.129 LEN=40 TOS=0x00 PREC=0x00 TTL=122 ID=54098 PROTO=TCP SPT=443 DPT=51165 WINDOW=0 RES=0x00 RST URGP=0 MARK=0x1
May  7 04:02:51 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=172.217.4.234 DST=216.160.2.129 LEN=40 TOS=0x00 PREC=0x00 TTL=122 ID=54121 PROTO=TCP SPT=443 DPT=51170 WINDOW=0 RES=0x00 RST URGP=0 MARK=0x1
May  7 04:02:52 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=185.176.26.100 DST=216.160.2.133 LEN=44 TOS=0x08 PREC=0x20 TTL=241 ID=61662 PROTO=TCP SPT=45013 DPT=17239 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:02:56 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=175.213.137.116 DST=216.160.2.134 LEN=44 TOS=0x00 PREC=0x00 TTL=47 ID=28046 PROTO=TCP SPT=23653 DPT=23 WINDOW=30789 RES=0x00 SYN URGP=0 MARK=0x1
May  7 04:03:01 localhost kernel: IN=br0 OUT= PHYSIN=eth0 MAC=00:10:4b:97:9b:38:a0:a3:e2:63:de:20:08:00 SRC=83.169.197.13 DST=216.160.2.129 LEN=44 TOS=0x00 PREC=0x00 TTL=236 ID=45109 PROTO=TCP SPT=50371 DPT=445 WINDOW=1024 RES=0x00 SYN URGP=0 MARK=0x1
```

# Awareness



“I don’t have time for this. Just tell me what I need to know in 25 words or less.”





# Everything busy leaders need to know about cyber-security

Distilled into a six word rhyme anyone can remember.

**Care and share to be prepared.**

Everything flows from that.



# Care!!

**Message to busy business leaders:**

- Pay more than lip service.
- Or enjoy the consequences of the next incident.

“We take security seriously.”

# Share

*A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks **offers a premium for dishonesty, by shewing others how to be dishonest. This is a fallacy.** Rogues are very keen in their profession, and they know already much more than we can teach them respecting their several kinds of roguery. **Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves,** as they have lately done. If a lock—let it have been made in whatever country, or by whatever maker—is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to be the first to apply the knowledge practically; and **the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.***

Alfred Charles Hobbs, “[Rudimentary Treatise on the Construction of Locks](#),” edited by Charles Tomlinson, published in 1853, page 2.

Also see <https://www.dgregscott.com/a-radical-not-so-new-idea-to-stop-the-daily-barrage-of-data-breaches/>



# Which do you prefer?

Embarrassment during peer reviews with other good guys?

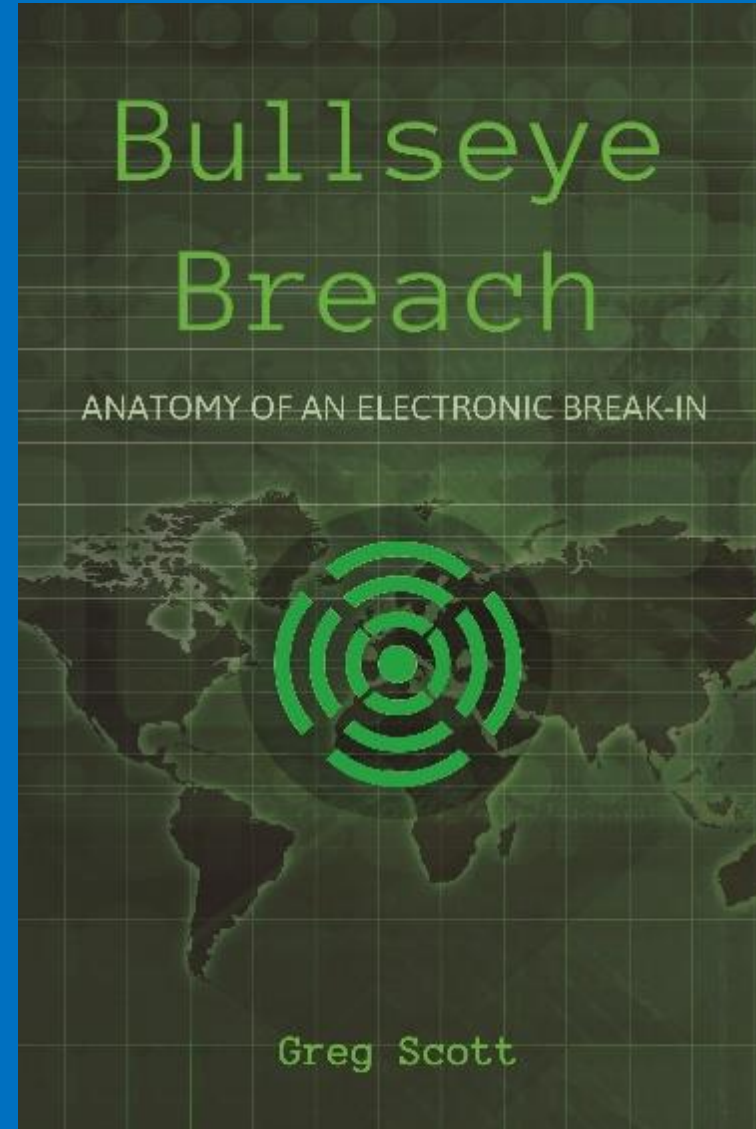
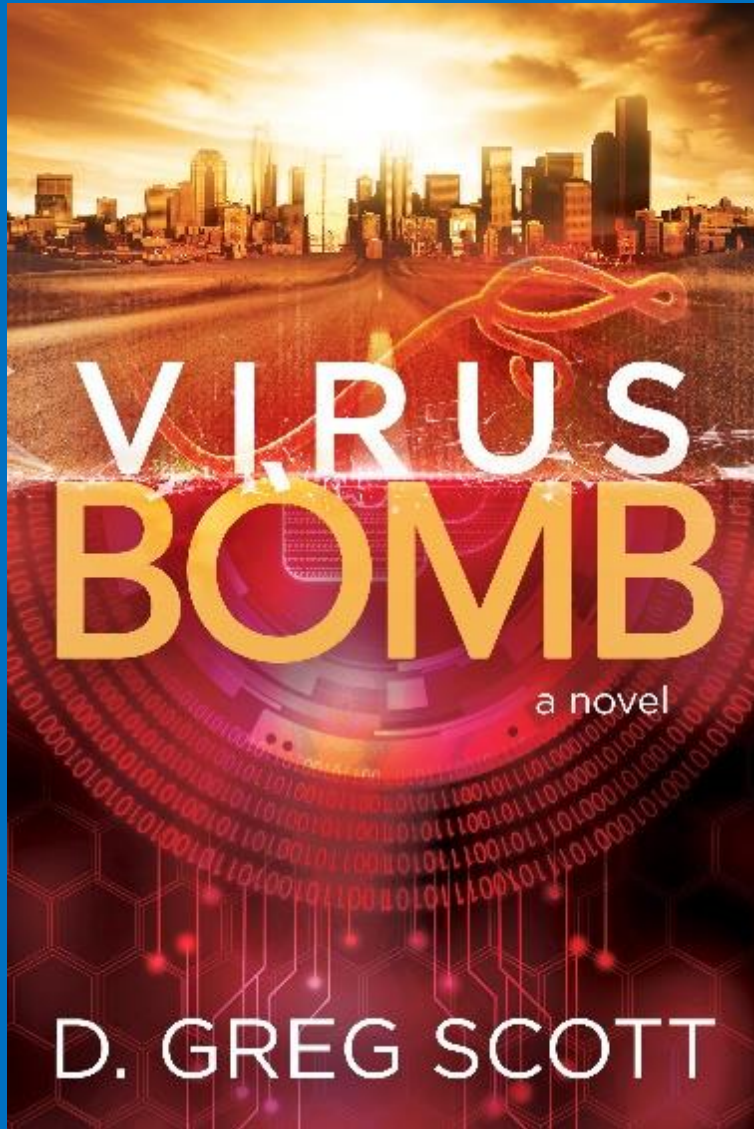
Or...

Embarrassment or worse in front of the whole world after somebody plunders you?

I practice what I preach. See

<https://www.dgregscott.com/time-to-man-up-swallow-my-pride/>

# Two Great Books

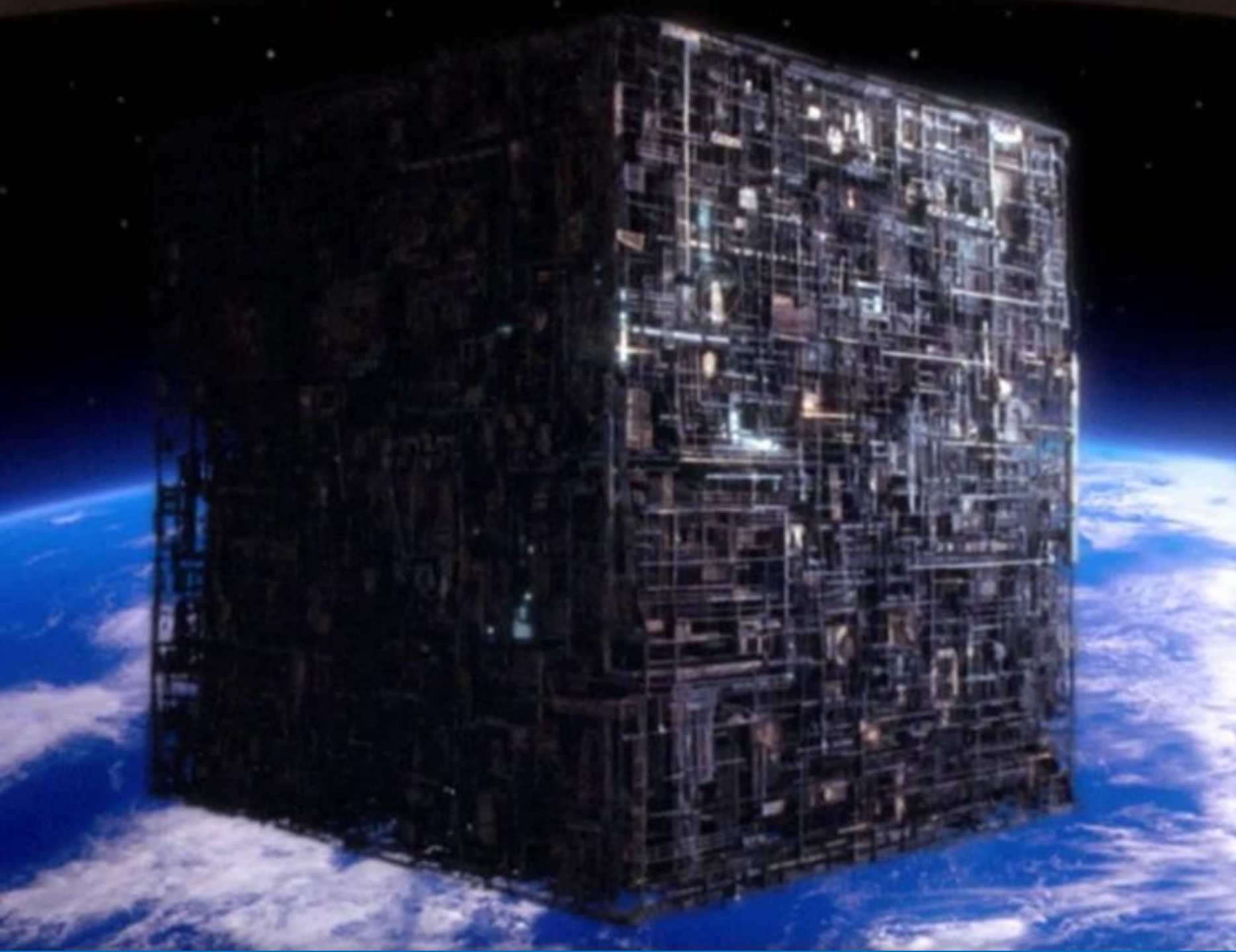


# Security is a process, not an event

- Share what you learn with other good guys.
- ~~Expect~~ Demand other good guys share what they learn with you.
- Apply what you learn; repeat and refine continuously.

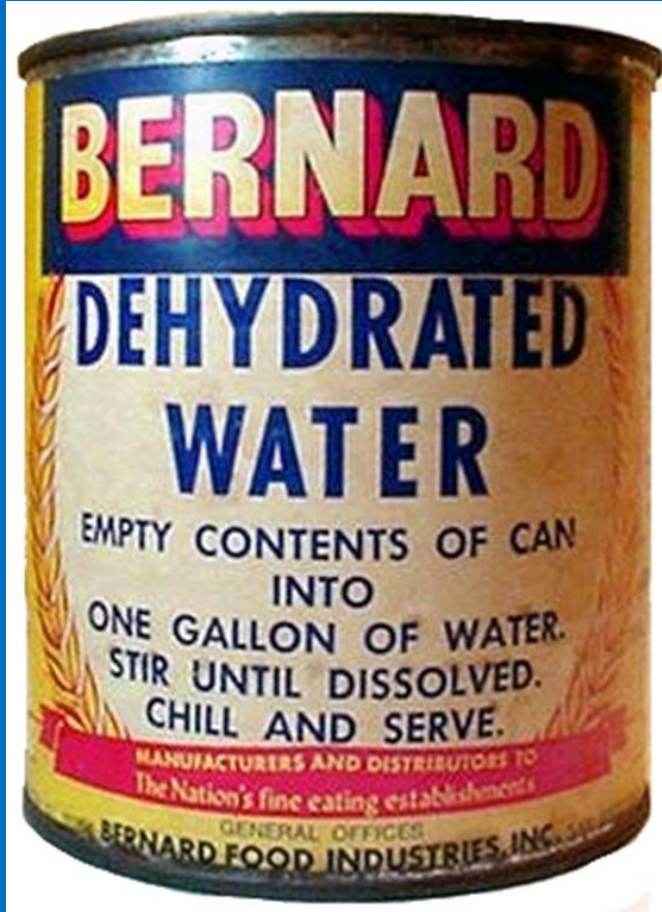
**Security is a process, not an event.**





Resistance  
is not futile.

# Con games are alive and well today and live on the Internet



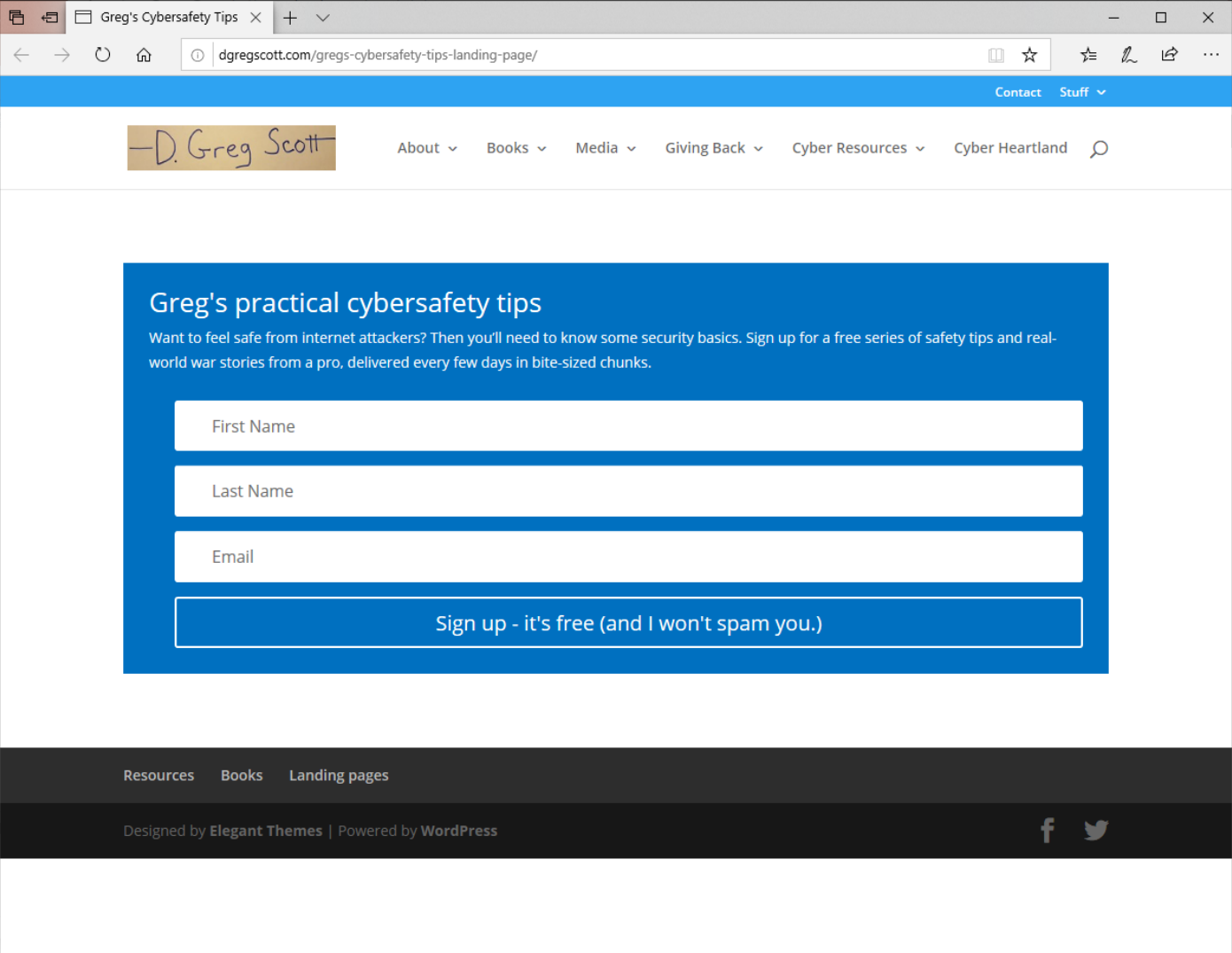
For a great satire blog post, see:

<https://www.dgregscott.com/social-media-mobs-not-just-fringe-groups-any-more/>

# One more plug

To opt in and get these tips delivered to your inbox:

- Go to my website
- Click the *big red* button
- Fill out the form



The screenshot shows a web browser window with the address bar displaying "dgregscott.com/gregs-cybersafety-tips-landing-page/". The website has a blue header with a navigation menu including "About", "Books", "Media", "Giving Back", "Cyber Resources", and "Cyber Heartland". A blue box in the center contains the title "Greg's practical cybersafety tips" and a paragraph: "Want to feel safe from Internet attackers? Then you'll need to know some security basics. Sign up for a free series of safety tips and real-world war stories from a pro, delivered every few days in bite-sized chunks." Below this is a form with three input fields labeled "First Name", "Last Name", and "Email". At the bottom of the form is a large blue button with the text "Sign up - it's free (and I won't spam you.)". The footer of the website includes links for "Resources", "Books", and "Landing pages", along with social media icons for Facebook and Twitter, and the text "Designed by Elegant Themes | Powered by WordPress".

Greg's Cybersafety Tips

dgregscott.com/gregs-cybersafety-tips-landing-page/

Contact Stuff

D. Greg Scott

About Books Media Giving Back Cyber Resources Cyber Heartland

Greg's practical cybersafety tips

Want to feel safe from Internet attackers? Then you'll need to know some security basics. Sign up for a free series of safety tips and real-world war stories from a pro, delivered every few days in bite-sized chunks.

First Name

Last Name

Email

Sign up - it's free (and I won't spam you.)

Resources Books Landing pages

Designed by Elegant Themes | Powered by WordPress

f t

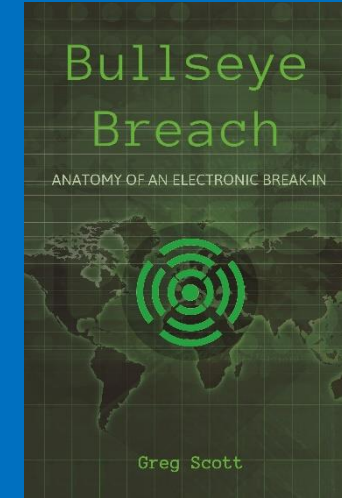
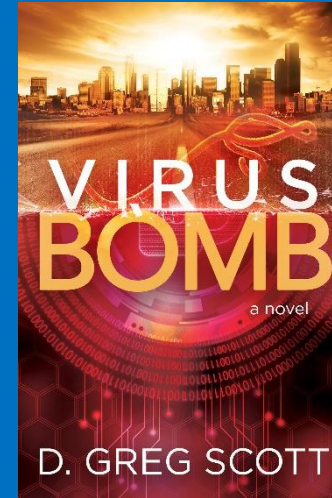


# Contact info

—D. Greg Scott

[gregscott@infrsupport.com](mailto:gregscott@infrsupport.com) or  
[gregscott@dgregscott.com](mailto:gregscott@dgregscott.com)

<https://www.dgregscott.com>



Twitter: DGregScott

LinkedIn: <https://www.linkedin.com/in/dgregscott/>

Facebook: <https://www.facebook.com/D-Greg-Scott-author-112197323547623>

Youtube: "Greg Scott Public Videos" at  
[https://www.youtube.com/channel/UCBtDWsqzMZ\\_RB94I\\_F4cnRQ](https://www.youtube.com/channel/UCBtDWsqzMZ_RB94I_F4cnRQ)