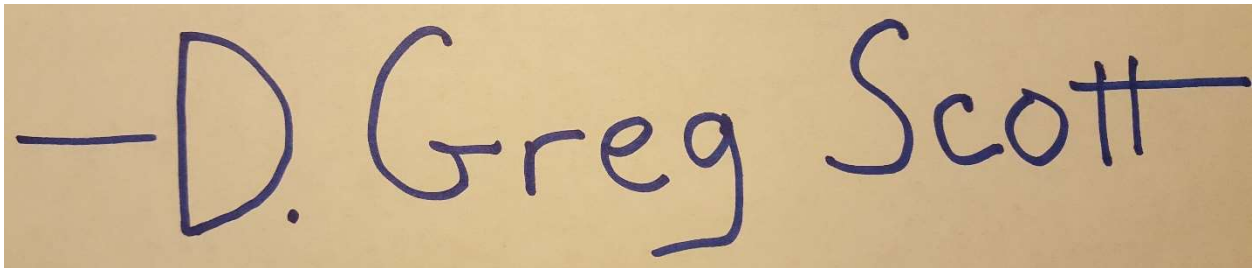


Greg's Practical Internet Safety Tips

A photograph of a piece of brown paper with the name "D. Greg Scott" written in blue ink. The signature is written in a cursive, handwritten style.

D. Greg Scott

gregscott@dgregscott.com

© 2019 by D. Greg Scott. All rights reserved.

Internet safety is like toilet paper. Nobody cares until there's an outage.

—D. Greg Scott

The internet, with its promise to democratize access to information, exposes all of us to unprecedented opportunities and threats. These threats are real, they're significant, they're personal, and they will hurt the unprepared. We need to prepare.

Preparing for those threats is a process, not an event. We don't achieve cyber-safety by buying a shiny new tool or service. We do it by maintaining awareness and getting lots of little things right.

Every month, hundreds of cyberattacks make the news. Nobody knows how many thousands don't make the news. Every single one, from the largest sensational headline, to the smallest family computer compromise, is preventable.

Here are some tactical tips to help avoid becoming a cybervictim.

Contents

- Email hygiene 1
- Patching 3
- Authentication—Prove You're You 5
- Trust 7
- Passwords and Passphrases 9
- Backups 11
- Social Media 13
- Mobility 15
- Tech Tools 17
- Awareness 19
- Six Words to Summarize Everything You Need to Know 21
- Read These Books 23

Email hygiene



Phishing – when a con-artist “phishes” for victims—is far and away the most common attack over the internet. An attacker sends a malicious email to a victim and persuades the victim to open an attachment or visit a compromised website. After the victim bites, the attacker owns the victim computer, tablet, or cell phone.

Spear-phishing is when a con-artist tailors a solicitation specifically for a victim. Spear-phishing is scary because it means somebody did homework on that victim. See *Social Media*, below.

One of the best phishing war stories is the one about Hilary Clinton's campaign manager, John Podesta, and the Democrats in 2016. Podesta opened an email claiming to come from Google and it said he needed to reset his Gmail password. He followed the link, logged into what he thought was Google, and gave Russian attackers his email password. And that was one link in a chain of events that led to the Democrats airing their dirty laundry on Wikileaks.

Poor email hygiene is on both sides of the political aisle. Apparently, Colin Powell, Republican former Secretary of State, also fell for a similar scheme.

Phishing attacks are successful because anyone can impersonate anyone else in an email. It’s an architectural weakness from the dawn of the internet. There are lots of proposals to address this problem, but nobody has a foolproof solution and none are coming in the foreseeable future.

Don’t trust emails claiming to come from your bank or your best friend. Don’t open attachments unless somebody you trust looks you in the eye and promises

the attachments aren't malicious. Hover over links and make sure they point where they claim to point before following them.

Here are a few links for more information:

- How to spot a phishy email from a mile away:
<http://dgregscott.com/week-2-day-2-spot-phishy-email-mile-away/>
- How to spot a phishy email
<http://dgregscott.com/spot-phishy-email/>
- Spam and phishing: Recognizing phishing scams:
<http://dgregscott.com/spam-phishing-mini-seminar/>

You probably don't keep national security secrets in your computer. But you do keep information important to you, and if you fall for a phishing scheme, somebody else will own you, your devices, and all the information inside. Don't be a victim. Do be smarter than politicians who should know better.

For your own protection, learn how to spot phishy spam emails and learn how to decipher email headers. Don't hide behind, "I'm not technical," because identity thieves prey on the unprepared.

Patching



Every piece of non-trivial software has bugs. Which means, the Mac vs. Windows vs. Linux computer security arguments, and the Android vs. IOS cell phone and tablet security arguments, are all a waste of time. They're all computers, they all do the same stuff, and attackers have found vulnerabilities in all of them.

Teams of researchers make lots of money finding vulnerabilities, teams of attackers make lots of money exploiting them, and software vendors put lots of energy into fixing them with updates.

When attackers fool victims into running malicious programs, those programs usually attack a recently patched vulnerability. Attackers hope victims never applied the update to fix the problem; and too often, they win.

Patching is always annoying. Windows might be the most annoying of all because it forces people to apply updates right now upon shutdown. This creates uncomfortable situations.

One time, I was in downtown Chicago on business and my Windows laptop decided to update itself right then and there before shutting down. I ducked into a bank lobby and sat on a bench for forty-five minutes watching it grind before jumping on the L to the airport. I barely made my flight home.

Another time, I was driving and set my laptop in the passenger seat to grind through an update. Bouncing around in the car while updating was a mistake, and my laptop hard drive paid the price. Which proves even IT professionals sometimes make dumb IT choices.

Patching doesn't need to be so annoying and I wish Microsoft would address it. In the meantime, if it's inconvenient to update your laptop right now, here's a trick. Close all your windows, and then click or tap the Start button and type "cmd" in the box. Inside the black command window that comes up, type:

```
shutdown /s
```

This will shut down your laptop right now without applying any patches. But when you get home, make sure you apply those patches. Let the update run overnight if you want to minimize the inconvenience.

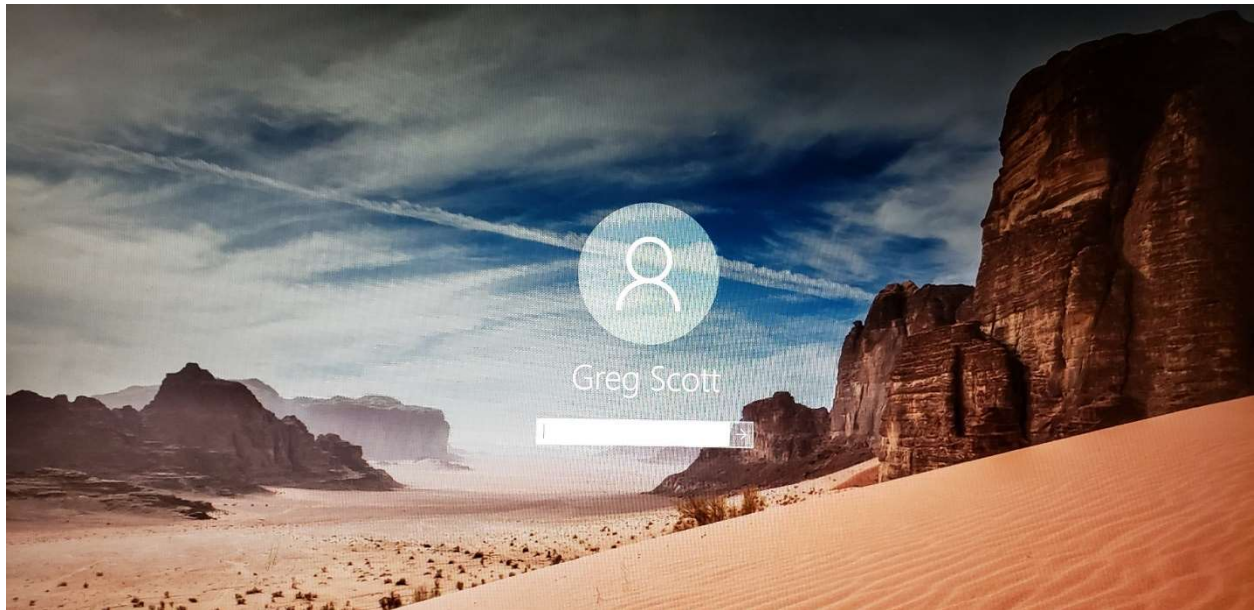
Here are links to more information.

- Why You Should Patch your PCs and Server Computers
<https://www.spiceworks.com/it-articles/patch-and-update-pc-and-server-computers/>
- Apple Security Updates
<https://support.apple.com/en-us/HT201222>
- How Important are Android Security Patches?
<https://www.androidcentral.com/how-important-are-android-security-patches>
- The Congressional Report on the Equifax Hack
<https://www.sans.org/security-awareness-training/blog/just-released-congressional-report-equifax-hack>

Poor patch management played a role in both my novels. The real world is full of stories about home computers, major corporations, and everywhere in-between penetrated because of poor patch management. When software updates come for your devices, apply them. If the updates have problems, troubleshoot and fix them. If you fail to apply a patch to a known vulnerability and somebody exploits it and steals your identity, it's your fault, not the vendor's. Don't become another statistic because you didn't apply the patches delivered to you.

—D. Greg Scott

Authentication—Prove You're You



We need authentication over the internet to make sure we're dealing with the person or organization we think we're dealing with, and not an impersonator.

Every authentication choice comes with tradeoffs. Fingerprints, eye scans, and other biometrics are promising, but, so far, expensive and unreliable. Passwords are a hassle to remember – see *Passwords and Passphrases*. And just say no to implanted RFID tags.

State of the art today is two-factor-authentication, or 2FA. With 2FA, if you want me to believe you're you, and not somebody impersonating you, then show me something I know only you have, and recite a secret only we know.

We usually implement 2FA with passwords and cell phone text messages. We both know your password, and you have a cell phone number. You send me a password—something we know—and then I send a code to your cell phone. You send me the code back to prove you have the cell phone. Encourage all online vendors to use 2FA.

But what about person to person authentication? How do you know that suspicious-looking social media post or email really came from your best friend? One great test—and this doesn't appear in any official how-to documentation—is a bogus challenge. Let's say Bob and Alice met in Chicago five years ago. Bob sees a social media post claiming to come from Alice, but Bob is suspicious. Bob might challenge Alice and ask what they had for dinner when they first met in New York

last year. If Alice really is Alice, she'll respond that they met in Chicago, not New York, and it was five years ago and she doesn't remember what they had for dinner. The trick is, ask a challenge question for which the only correct answer is, it's a bogus question.

One time, somebody hijacked my half-brother, David's email account and sent out some strange emails. David found out about it and sent out an apology to all his contacts. But I wasn't sure if David really sent it. And so I challenged him. I asked him our mother's maiden name. We have the same father, different mothers, and so my challenge was bogus. His answer convinced me he really was David. There's nothing high-tech about this tactic, and it might come in handy if somebody claiming to be a grandson stuck in an overseas jail contacts you and begs for money.

Here are links to more information.

- Two Factor Authentication: Who Has it and How to Set it Up
<https://www.pcmag.com/feature/358289/two-factor-authentication-who-has-it-and-how-to-set-it-up>
- Never allow an RFID tag implanted in your body
<http://dgregscott.com/nuts-never-let-anyone-put-rfid-tag-inside-body/>

Do use two-factor authentication whenever possible. Something you know and something you have is stronger than just something you know. Don't fall for impersonators who want to steal your money and your identity.

Trust



People have spread lies and rumors since the dawn of people. But today we can zip lies around the planet in seconds. Don't lose your wits just because you read it on the internet. Do use courtesy when interacting on the internet. Real people are on the other side of those conversations.

I saw a breathless TV news story from a consumer reporter in California back in 2017 about - queue the horror music - somebody impersonating Amazon. The story generated thousands of online comments, including mine, asking what was the big deal because not a day goes by without somebody trying to impersonate Amazon or any number of online retailers.

Trust also has a technological dimension. In addition to mutual authentication, we need a way to trust what other parties tell us. We trust websites such as Amazon, Google, and others because we implicitly trust third party certificate authorities who make money from attesting these websites are legitimate. The public should understand how this works.

Here are links to more information.

- How trust on the internet works:
<http://dgregscott.com/internet-trust-mini-seminar/>
- How to fix the credit reporting system:
<http://dgregscott.com/143-million-reasons-credit-reporting-industry-reform-part-2/>

Trust violations can cost you money, scramble your files, destroy your reputation, influence national elections, and change global events. Apply due diligence to anything you read on the internet, and learn how trust on the internet really works.

—D. Greg Scott

Passwords and Passphrases



Every time my wife logs into any website, she has to go through the forgotten password procedure. She swears the websites are messed up and complains every day about how inconvenient all these passwords are. She's partially right; passwords are inconvenient, and keeping different passwords for different websites is even more inconvenient. But the alternative is worse. Much worse.

Unlike Hollywood hacker scenes, complex passwords using random strings of UPPPER case, lower case, and special characters are hard to guess and hard to attack with brute force or dictionaries. But they're also hard to remember.

Passphrases are better than passwords because they're easier to remember and even harder to guess or brute force attack.

Consider this string of ten random characters, including upper case, lower case, and special characters: *h4GehD\$jH%*. And now consider this pass phrase:

ilikepassphrases. Which is easier to remember? And which is harder to guess? You can do your own calculations; but the passphrase wins.

Unfortunately, most website operators haven't gotten the message yet, and they still want complex passwords. Accommodate them using complex passwords like this: ILikeP@ssphrases.

Keep passwords/passphrases somewhere safe, and never inside your computer, cell phone, tablet, or other device.

Don't use the same password/passphrase for banking as you use for social media. It's inconvenient to keep separate passwords for everything, but it's worse when somebody drains your bank accounts after stealing your Instagram password.

Here are links to more information:

- Passwords must die: Long live passphrases
<http://dgregscott.com/passwords-must-die-long-live-passphrases/>
- Hollywood hackers—Guess the password, save the world
<http://dgregscott.com/hollywood-hackers/>
- More on Hollywood hackers
<http://dgregscott.com/week-4-day-1-hollywood-hackers-lets-do-better/>

Good password practice is like good diet and exercise. We might not enjoy it, but it helps keep us alive.

Backups



I tell new IT people, they aren't professionals until they've destroyed somebody's critical data and there's no recovery. My time came in 1981 and my first IT job at a small engineering college in Terre Haute, Indiana.

Computers were the size of refrigerators in those days. It was a busy time and I hadn't done backups in four weeks. I took down the Registrar's Office removable disk and mounted it on the larger system with a tape drive and started copying. A couple minutes later, the heads crashed and destroyed the Registrar's disk. I lost all the Registrar's Office data when the heads crashed, and all the backup data on tape because I had to initialize it before starting my copy operation. In one move, I destroyed every piece of online data from the Registrar's office.

It was uncomfortable when I had to explain what happened and why. It took months to recover the data. My reputation never recovered.

Like most IT professionals, I could fill a book with war stories around backups. Here's a link to one story from 2014. I call it my Apollo Thirteen moment. And practice hovering over this link to make sure it points where it claims to point.

<http://dgregscott.com/business-continuity-disaster-recovery-apollo-13-week/>

Hardware problems, software bugs, mistakes—any number of things can destroy your data in a heartbeat. Add to those well-known challenges a new class of threats: ransomware.

A ransomware attack is a 21st century shakedown scheme where somebody scrambles all your files and then offers to unscramble them for a fee.

If you're a consumer, imagine somebody scrambling your past five years of tax records the day before an audit. Or 20,000 photos and videos, including memories you wanted to preserve about your overseas vacation.

If you're a business, imagine losing every scrap of information your business needs to operate. These days, most of it is inside a computer.

After a successful ransomware attack, only two recoveries are possible; restore your information from backup, or pay the ransom and put more money into criminals' pockets. The local police, the FBI, the CIA, the NSA, and the Department of Homeland Security can't help you.

One more challenge: if your systems know where their backups live, so does malicious software inside those systems. Guard against this by putting another system between your computer(s) and your backups, and use it only for backups. Set it up such that it can reach inside your computer, but nothing can reach inside it.

Here are links to more information.

- <http://dgregscott.com/business-continuity-disaster-recovery-apollo-13-week/>
- <https://www.bostonglobe.com/business/2015/04/06/tewksbury-police-pay-bitcoin-ransom-hackers/PkcE1GBTOF52p31F9FM5L/story.html>

Keep good backups. Or risk what happened with the Tewksbury, MA. Police department. Or the city of Atlanta. Or thousands of other people and organizations who failed to protect themselves.

Social Media



Facebook, Instagram, LinkedIn, Twitter, YouTube, and others offer more ways for people to connect than ever in history. And all for no money. But it's not free.

Unfortunately, our privacy conflicts with their business model, and this leads to problems.

Facebook is fighting multiple scandals about its cavalier attitude to its users' privacy. LinkedIn lost millions of user passwords a few years ago. Yahoo lost three billion user passwords and took years to disclose it. Google owns YouTube and tracks every movement it can for people who use it.

The bigger the audience, the more money social media companies make. So, they recruit us to contribute free content they can slice and dice and sell to marketing companies. All social media companies sell the information they collect to anyone willing to pay.

Assume the whole world will see everything you post on social media. Even if your settings say private, you're trusting people who sell your information as a revenue model to keep it private. Share your deepest feelings with that in mind.

As an author, I've done public posts about uncomfortable topics. One time, I started a thread about how to hijack GPS signals and hijack trucks. I did another one about how to set up a cell phone bomb detonator. Usually, when I start a thread like that, somebody eventually comments that I'm likely on a government watchlist. I always reply with something like, "for the dedicated law enforcement professionals following this thread, you need to buy a copy of my books for everyone in your department, your supervisor, and your supervisor's manager. And do it quickly, because my books contain my manifesto to take over the world and you need to read them before it's too late."

Here are links to more information.

- Why social media is good:
<http://dgregscott.com/whats-good-about-social-media/>
- Why social media is bad:
<http://dgregscott.com/week-3-day-2-why-social-media-is-bad/>

Use social media with your eyes open, because we're not customers, we're raw material. No matter how many promises anyone makes, it's a conflict of interest when a company whose revenue model depends on selling our content promises to keep it private. Trusting a social media site with your most intimate secrets could cost you your job or turn you into an identity theft statistic. Or worse.

Mobility



Just like an earlier generation embraced automobiles, today we're embracing smartphones. How did we ever get along without them?

The security challenge is, all those "free" mobile apps come with a cost. The Snowden revelations of 2013 exposed government agencies tracking our calls and data usage. But an entire industry of marketing companies make money by tracking more about us than the most intrusive government surveillance. And we volunteer for it.

But it's not always sinister. Sometimes it's a tech glitch.

One time, my daughter was trading text messages with another mom to set up a play-date for my grandson. The other mom offered to have my grandson over to her house to play with her son, and my daughter offered to stay and help. This was one of my daughter's messages:

"Sounds good. I am cool with staying and hanging out if you want. I just don't want you to feel like overwhelmed or anything."

The other mom responded and they continued their text conversation.

In the middle of her conversation with the other mom, two identical text messages from two different unknown local phone numbers came in. The messages were, "who dis?" followed by forwards of my daughter's messages to the other mom.

How did some lowlife intercept her text messages and play them back for her? What did they want?

I texted one of the numbers with “who are you and what do you want?” A few seconds later, her phone rang with the caller-ID from the first number.

The caller was a woman and she was just as mystified as my daughter. She said she received a text message about staying and hanging out from this number, but had no idea what that meant or what was going on. She knew my daughter’s name because my daughter used it in another message in the conversation thread. How did this unrelated third party end up with a copy of part of my daughter’s half of a conversation with the other mom?

Curious, we called the other number. That was also a woman, but she thought my daughter was a guy sending inappropriate advances. What does “hang out” really mean anyway? We had a long talk and cleared it up.

Apparently, T-Mobile, had a text message routing problem that day and sent copies of text messages to unintended phone numbers. There was no cyberattack, no stalkers, no perverts. Just a tech glitch with suspicion layered on top.

Many mobile apps’ real purpose is spying. Protect yourself. Only install mobile apps from approved Apple or Android stores. And pay attention to the permissions apps demand. For example, why does a flashlight app need access to your contacts?

Here are links to more information.

- Top 5 Cell Phone Spy Apps
<https://bestcellphonespyapps.com/>
- Spy on Cell Phone Without Installing Software on Target Phone
<https://celltrackingapps.com/how-to-spy-on-cell-phone-without-having-access-to-the-phone/>
- These Academics Spent the Last Year Testing Whether Your Phone Is Secretly Listening to You
<https://gizmodo.com/these-academics-spent-the-last-year-testing-whether-you-1826961188>

Today’s mobile infrastructure gives us ways to connect that only existed in science-fiction a few years ago. Make sure nobody uses your mobile devices to spy on you.

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=216.160.2.1
33 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=216.160.2.1
29 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=216.160.2.1
29 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=216.160.2.13
6 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=216.160.2.1
29 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=216.160.2.12
9 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=216.160.2.1
36 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=216.160.2.12
9 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=216.160.2.12
9 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=216.160.2.1
33 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=216.160.2.12
9 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
```

Plenty of technology tools are available to help protect against all classes of threats. Firewalls keep unsolicited traffic out, antivirus subscriptions help guard against malicious software implanted in our devices, spam filtering helps keep out phishing attacks, outbound web filtering helps help keep us away from malicious websites, and artificial intelligence systems are becoming available to help sniff out suspicious traffic entering our networks and devices.

I spent fifteen years building firewalls. I built hundreds over the years, and every time I connected one to the public internet, within about five seconds, I saw automated probes from around the world targeting my system and the network behind it. When I say bad guys have plenty of automation looking for vulnerabilities, I speak from experience.

There was nothing secret or proprietary about my stuff. I used the latest version of Red Hat Fedora with relevant packages and an iptables script. For hardware, I started with used PCs and fought all the problems with used PCs until I found a more compact new platform.

And I routinely used off-the-shelf tools to track down virus-infested computers and users abusing internet connections. To this day, I haven't seen anything with

-D. Greg Scott

better diagnostics at the network boundary than the open source packages I found.

In both my novels, Jerry Barkley uses similar tools to track down cyberattacks. I won't spoil the stories with details here; enjoy the books.

With the rise of internet-connected thermostats, kitchen appliances, door locks, security cameras, sensors, and other IoT (Internet of Things) devices, millions of consumers now host little websites in their homes. And just like their bigger cousins in commercial hosting centers, armies of automated attackers probe these IoT devices every few seconds, all day, every day. This means every home needs an upgraded firewall at its internet boundary with diagnostic tools to recognize and block these probes.

Here are links to more information.

- <https://bestcompany.com/identity-theft/blog/how-to-make-smart-choices-for-your-smart-home-part-1>
- <https://bestcompany.com/identity-theft/blog/how-to-make-smart-choices-for-your-smart-home-part-2>

As technology advances, security automation tools will play an ever-more important role keeping us safe on the internet, because automation can do a better job of watching traffic and possibly preventing malicious activity than any human. Make smart choices on what security automation to buy and how to use it.

But relying solely on automation is a fatal mistake.

Awareness



No security automation technology will ever be one hundred percent effective. People will *always* be the last and best line of defense against attack. Which means we need to always be aware of what's going on around us. Think of it as the equivalent of walking through a downtown late at night.

In "Virus Bomb," when Jerry Barkley tries to tell Sally Brock about the cyberthreats she's up against, she blows him off. Repeatedly. Sally is a composite character representing dozens of people I've met over the years who purposely close their eyes to cyberthreats. "Bullseye Breach" has a whole management team in denial.

A few "Virus Bomb" beta readers commented nobody in real life is this unaware. Those beta readers were wrong. I remember a bank vice-president who refused to acknowledge the difference between his bank internal network and the bank website. And a dentist who kept his patient X-ray images on a Windows XP system in a dusty cubicle and never backed it up. When I asked him what would happen if

he lost all those images, he said he didn't need computers to do dentistry. Then there was the store owner who didn't want to clean the viruses from the store computer she shared on the public WiFi with her customers. And dozens of home computer users with devices polluted with thousands of viruses, downloaded from who-knows-where. Plenty of people spend too much time in denial and need to wake up.

Never trust any technology over old-fashioned human judgment. Don't believe pitches for any products or services that claim to solve all your security problems. That artificial intelligence showing all that potential to protect you? Attackers use the same artificial intelligence to attack you.

With every website, every email, every interaction over the internet, learn how to think like an attacker. Develop a habit of asking how an attacker might use this interaction to fool a potential victim into doing something thoughtless, and then evaluate the risk and alternatives.

Here are links to more information.

- Hollywood's warped view of cybersecurity
<http://dgregscott.com/hollywood-hackers/>
- An identity theft scheme with no technology defense:
<http://dgregscott.com/steal-identity-fun-profit/>
- Myths about Russian hackers and cheap internet routers.
<http://dgregscott.com/russian-hackers-internet-router-fairy-tales/>

People are the most vulnerable link in the cybersecurity chain. But as the last line of defense, people are also the most important link. We *must* maintain awareness. Similar to learning what the gas pedal steering wheel, and brakes do, learn what IP Addresses, DNS servers, switches, and routers do. This knowledge will help save you from an identity theft nightmare. Or worse.

Lots of people pay a steep price for cybersecurity failures. That's why I wrote my novels. You don't need to make the same mistakes.

Six Words to Summarize Everything You Need to Know



One time, a busy organization leader asked me about how malicious software gets onto his computer. I started to answer and he interrupted me in mid-sentence. "Greg, just tell me what I need to know in twenty-five words or less." I walked away mad. Just jump off the cliff and learn on your way down.

But this doesn't do any good, and an answer worked its way into my brain a few months later. A deeper level of perspective can give busy organization leaders what they want with words to spare.

For people too busy to dig deep, or who think cybersecurity is somebody else's problem, commit this six-word rhyme to memory:

Care and share to be prepared.

Those six words summarize everything everyone needs to know about cybersecurity.

Care enough about your own cyber-safety to do something about it. Even though you don't keep information anyone cares about, attackers still want to use you to hit somebody they do care about. Don't be a drone.

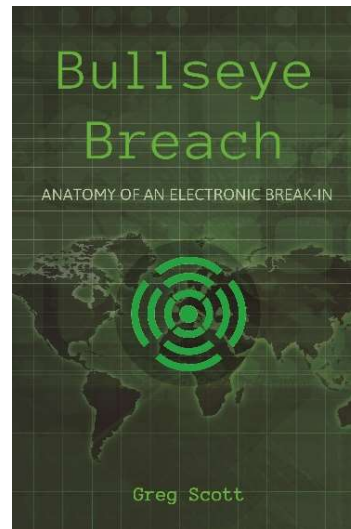
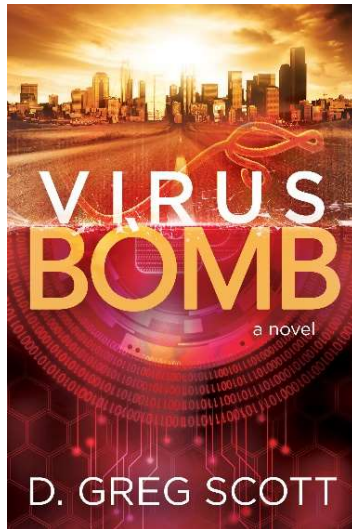
Share what you learn. Liberally. Other people can learn from your experience. And you can learn from others' experiences.

Here are links to more information.

- You don't need to be a cybervictim.
<http://dgregscott.com/30-day-challenge-week1-day1/>
- Our political leaders set sorry cybersecurity examples.
<http://dgregscott.com/political-leaders-set-sorry-security-example/>
- Care and share to be prepared part 1:
<http://dgregscott.com/care-and-share-to-be-prepared-part-1-caring/>
- Care and share to be prepared part 2:
<http://dgregscott.com/care-and-share-to-be-prepared-part-2-sharing/>
- Why it's important to share:
<http://dgregscott.com/week-1-day-5-cybersafety-care-and-share-to-be-prepared-why-is-sharing-important-watch-and-find-out/>

Bad guys spend all day probing good guys and all night collaborating on how to improve their probes for the next day. Good guys need to level the playing field. Especially good guys who don't know anything about technology. It *is* worth your time to learn.

Read These Books



The biggest problem with cybersecurity is, most people think it's complicated and boring. Like any profession, it does have its tedious moments. I've had my share of trouble staying awake through thousands of pages of documentation and preparing for tests.

But winning against cyberattackers is a fascinating combination of technology and psychology. The best cybersecurity professionals are some of the most creative and dedicated people I've had the privilege of meeting. We need more cybersecurity good guys, because plenty of bad guys want to plunder us.

It's a time-honored tradition to use fiction to present truth better than the news, and by 2014, I was frustrated with headline after headline about companies who allowed attackers to steal my personal information. Every single one of those data breaches was preventable, and so I decided to do something about it.

I published *Bullseye Breach: Anatomy of an Electronic Break-In* in 2015 to show how Russian mobsters stole 40 million customer credit card numbers from fictional retailer, Bullseye Stores, and what an ad-hoc team in Minneapolis did about it. In 2019, I published *Virus Bomb* to show what might happen if a nation-state really does get serious about attacking our country over the internet.

Here are links to more information:

- Virus Bomb
<http://dgregscott.com/virus-bomb/>

- Bullseye Breach: Anatomy of an Electronic Break-In
<http://dgregscott.com/bullseye-breach/>
- Good guys, bad guys, and victims
<http://dgregscott.com/a-few-people-from-the-bullseye-breach-and-virus-bomb-incidents/>

In the real world, just like my fiction, and whether we like it or not, all of us are on the front lines of the cybersecurity war. If good guys don't up our games, then bad guys will continue plundering us every day. Don't expect government cyber superheroes to protect us, because they can't. Real superheroes are ordinary people who step up when called. We're all being called.

