



HILLTOP

WEALTH SOLUTIONS

Special Online Event

Hosted by CEO Erik Brenner, CFP®, NSSA®

**Defending Against the Data Breach: Protect from
Spyware, Malware, Ransomware and Keyloggers** 



Defending Against the Data Breach:
Protect from Spyware, Malware,
Ransomware and Keyloggers
Robert Siciliano www.Safr.Me

15 Fundamentals of Data Protection



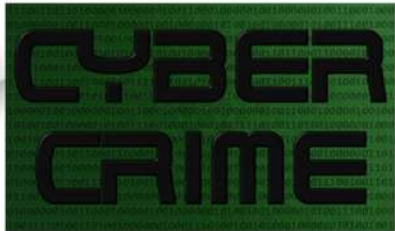
- **Have a Plan:** As the saying goes, “if you fail to plan, then you plan to fail”. But when it comes to data security “if you fail to plan, you plan to pay”. And that means you’re paying the bad guy or lawyers or the government in fines. Or you’re losing business because of a poor security reputation.
- **Social Engineering:** Know that every time the phone rings, an email comes in, or even an invoice via the US Postal Service is received, that the communication could be designed to socially engineer or influence you or a staff member to transfer money out of your bank account for one reason or the other. No matter the reason for the communication, it’s intensity, immediacy or threatening nature, the upmost scrutiny needs to be given before monies are paid. Just stop and think before taking action.
- **Security Awareness Training:** Whether it be hardware, software, or human hacking, there are always vulnerabilities in all systems, all around us. The only way to properly plug these various holes is through education both in person, virtually, and through phishing simulation training. This requires a little bit of time and expense and is an absolute necessity of doing business in 2020 and beyond.
- **Hardware:** Make sure your devices such as PC’s, laptops, mobiles, modems, routers and any peripherals are newer. Old hardware (5+ years) sometimes lacks internal resources to run current more secure software and firmware.
- **Secure Software:** Keep all devices operating systems updated with the latest software updates and critical security patches. Install and run a paid version of antivirus, anti-spyware, anti-phishing and a 2-way firewall.

15 Fundamentals of Data Protection



- **WiFi Security:** Set up a secure WiFi connection in your home or business.
- **VPN:** Ensure your laptop and mobile devices and its data are protected on open free WiFi by using a VPN or “virtual private network”
- **Encryption:** Protect your data with encryption software.
- **Tracking:** Install, set up and enable tracking software for lost or stolen laptops and mobile phones
- **Backup:** Back up and sync all your information on redundant internal and external local hard drives. Back up externally to cloud based backup sites. Back up all data on iPhone and Android mobiles.
- **Passwords:** Set up and run password manager software and eliminate password re-use by having a different password for every online account.
- **Two Factor:** Set up two-factor or two step authentication for any and all critical accounts that deploy it.
- **Social Engineering:** Recognize social engineering scams every time the phone rings, an email comes in or someone knocks on the door.
- **IT Vendors:** Use your circle of influence or trusted network to make recommendations when hiring IT security contractors such as virtual Chief Information Security Officers (vCISO), or depending on the size and scope of the organization a Managed Security Service Provider also known as in MSSP to ensure the security of your network.
- **Social media:** What you say, post, like, or share has repercussions. Manage your online reputation.

2017 Smashed Worlds Records for Most Data Breaches Ever!



Five Mega-breaches accounted for 72% of all data records exposed in 2017.

It was a record-breaking year for the numbers of publicly reported data breaches and exposed records in 2017 worldwide: a total of 5,207 breaches and 7.89 billion information records compromised.

More than 15.1 Billion Records Exposed in 2019



There were 7,098 breaches reported in 2019, a one percent increase on 2018, though the gap is anticipated to grow throughout Q1 2020 as more 2019 incidents come to light, says the new Risk Based Security report, [2019 Year End Data Breach QuickView Report](#).

The total number of records exposed in 2019 increased by 284 percent compared to 2018. In total, there were over 15.1 billion records exposed.

Google News

 a smart, secure and

Equifax Breach Affects 143 Million Customers



Equifax is just one of many thousands of data breaches. And its not even the biggest data breach. But it is the poster child for data breaches and here is why:

Equifax CEO and CIO are both GONE. Fired, no. Retired. Which means they collected fat paychex on their exit. Ever since the Target breach company officers and board of directors heads roll whenever another breach occurs.

Equifax "Chief Security Officer" who also retired has a bachelor's degree and a master of fine arts degree in music composition. And she had ZERO experience in security.

Train's C

Google News

 a smart, secure and

AN ASTONISHING 773 MILLION RECORDS EXPOSED IN MONSTER BREACH

772,904,991 unique email addresses, over 21 million unique passwords, all recently posted to a hacking forum.

Train's arrival in Beijing raises speculation of Kim visit

Google News Safr.me a smart, secure and

Hackers are stealing closing funds by intercepting lawyer-client email, experts say.

Hackers are intercepting email between lawyers and clients, as well as real estate agents and their clients. In an effort to steal closing funds.



Train's arrival in Beijing raises speculation of Kim visit

/haveibeenpwned.com/?version=meter+at+1&module=meter-Links&pgtype=article&contentId=&mediald=&referrer=&priority=true&action=c

Home Notify me Domain search Who's been pwned Pastes API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address or username pwned?

112	1,070,622,134	37,078	27,760,975
pwned websites	pwned accounts	pastes	paste accounts

Have I Been Pwned (Troy Hunt) [AU] | <https://haveibeenpwned.com/Passwords>

Home Notify me Domain search Who's been pwned **Passwords** API About Donate

Pwned Passwords

Pwned Passwords are half a billion real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online system. [Read more about how HIBP protects the privacy of searched passwords.](#)

password

Password reuse and credential stuffing

Password reuse is normal. It's extremely risky, but it's so common because it's easy and people aren't aware of the potential impact. Attacks such as [credential stuffing](#) take advantage of reused credentials by automating login attempts against systems using known emails and password pairs.

Password Security

a smart, secure and Safr.me

- ❖ Social engineering
- ❖ Phishing
- ❖ Password re-use
- ❖ Insecure/weak pass
- ❖ Password managers
- ❖ Two step verification
- ❖ NO PASSWORDs



[Redacted name]

1:01 PM

Hi Rob,

I'm not sure if you saw what had happened on my FB Page last night, but someone stole my cell phone while I was at a concert, and posted all of my naked pictures off of my phone and posted them to my wall.

They were up there for hours. 😞

Is there anyway you could help me find out who it was?

Protect Yourself From Social Engineering Scams

Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim.

THERE IS NO PATCH FOR HUMAN GULLIBILITY


- 🔒 Lose something
- 🔒 Gain something
- 🔒 Fear/greed
- 🔒 "Principles of Influence and Persuasion"
- 🔒 email
- 🔒 telephone
- 🔒 in person
- 🔒 Thieves pose as You
- 🔒 Spouse
- 🔒 Bill collector
- 🔒 Bank
- 🔒 Utility
- 🔒 Fellow employee
- 🔒 Government agency



Google News

People are Still Dumb Enough To Pick Up Abandoned USBs and Plug Them In!

Would you pick up and use someone else's dirty tooth brush?



Safr.me e smart, secure and

Secure | https://www.amazon.com/Original-USB-KeyLogger-8MB-Black/dp/B078LN4W6H/ref=pd_sim_147_2?_encoding=UTF8&pd_rd_i=B078LN4W6H



DataLogger

The Original USB KeyLogger 8MB Black

★★★★☆ 46 customer reviews | 26 answered questions

Price: **\$49.95 & FREE Shipping.** Details

Get \$50 off instantly: Pay \$0.00 upon approval for the Amazon Rewards Visa Card.

prime | Try Fast, Free Shipping

Only 4 left in stock - order soon.

Want it Thursday, Jan. 11? Order within **16 hrs 21 mins** and choose **Two-Day Shipping** at checkout. Details

Sold by **Vengeance Gaming** and Fulfilled by Amazon. Gift-wrap available.

- Saves Over 4000 Pages Of Text!
- 100% Undetectable
- Works Instantly! No Installation Needed!
- Works with Windows and Linux
- For Wired Keyboards

KeyLogger

Prevent Phishing Scams That Empty Bank Accounts



- ❖ Spray and Pray
- ❖ CEO fraud (BEC)
- ❖ Spear Phishing
- ❖ Social Media Phishing
- ❖ SMS Mobile Smishing
- ❖ Phishing Simulation training



Covid-19 Scams



Beware of these Pandemic Phishing Scams

- ❖ Cybercriminals continue to target victims, even in this environment, and many of these scams are related to COVID-19

Relief Fund Scams

- ❖ Criminals have started to create phishing scams that look identical to the correspondence that might come from the government. They do this to trick people into revealing their personal information.

Infection Maps that are Malicious

- ❖ Organizations like Johns Hopkins are creating these maps, but cybercriminals are following close behind and releasing their own.

Impersonating Official Health Organizations

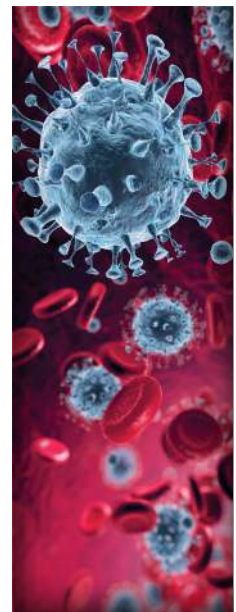
- ❖ Cybercriminals who are impersonating official health organizations, including WHO - the World Health Organization, or the CDC - Centers for Disease Control.

Scams with COVID-19 Testing Kits

- ❖ There is also a lot of interest in COVID-19 testing kits, and as you might imagine...the bad guys are targeting these people, too. Not only are these scams spreading via email, according to the FCC, Federal Communications Commission, but also with robocalls, text smishing, and more.

Medical Supply Scams

- ❖ These are similar to the testing kit scams but the cybercriminals are using these medical supplies, like masks and gloves, as a lure to get people to give them money.



Google News

a smart, secure and
Safr.me

93% of Phishing emails Are Now Ransomware

The skyrocketing growth is due to that fact that ransomware is getting easier and easier to send and that it offers a quick and easy return on investment.



New York Today: A Sunny Day at the Death Cafe
New York Times - 20m ago

Identity Theft **Frauds and Scams**

a smart, secure and
Safr.me



- ❖ **New Account Fraud** Using another's personal identifying information (SSN) to obtain products and services using that person's good credit standing.
- ❖ **Account Takeover Fraud** Using another person's account numbers such as a credit card number to obtain products and services using that person's existing accounts or extracting funds from a person's bank account.
- ❖ **Child Identity Theft** Studies show child identity theft is affecting over 1 million kids every year.
- ❖ **Tax Identity Theft** Tax-related scams hit \$240 million in 2017 with 109,000 victims. About 10,000 business returns have been identified by the IRS as potential identity theft.

Form **14039**
(April 2017)

Department of the Treasury - Internal Revenue Service

Identity Theft Affidavit

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting (Required)

- 1. I am submitting this Form 14039 for myself
- 2. This Form 14039 is submitted in response to a 'Notice' or 'Letter' received from the IRS
 - Please provide 'Notice' or 'Letter' number(s) on the **line to the right**
 - Please check box 1 in **Section B** and see special mailing and faxing instructions on reverse side of this form
- 3. I am submitting this Form 14039 on behalf of my 'dependent child or dependent relative'
 - Please complete **Section E** on reverse side of this form.
 - Caution:** If filing this on behalf of your 'dependent child or dependent relative', filing this form will protect his or her identity but it will **not** prevent the victim in **Section C** below from being claimed as a dependent by another person.
- 4. I am submitting this Form 14039 on behalf of another person (*other than my dependent child or dependent relative*)
 - Please complete **Section E** on reverse side of this form.

Section B - Reason For Filing This Form (Required)



HILLTOP

WEALTH SOLUTIONS

Thank You!

833.889.7526

info@hilltopwealthsolutions.com