SECURITY PROTOCOLS FOR AGENCIES, ORGANIZATIONS AND OUTSIDE PARTIES

Always remember: Anybody that does not like you can open, read and take any photo, data, email or text on EVERY phone, computer, network or electronic device you have ever used no matter how “safe” you think your personal or work system is! They can do this in less than a minute. Also: Hundreds of thousands of hackers scan every device, around the clock, even if they never heard of you, and will like your stuff just for the fun of causing trouble. Never use an electronic device unless you encrypt, hide and code your material!

If you are reading this notice, the following data applies to you:

1. Your network is known to contain Intel, Cisco, Juniper Networks, AMD, QualComm and other hardware which has been proven to contain backdoor hard-coded access to outside parties. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

2. Chinese, Russian FSB, Iranian and other state-sponsored hacking services as well as 14 year old domestic boys are able to easily enter your networks, emails and digital files because of this. They can enter your network at any time, with less than 4 mouse clicks, using software available to anyone. This is a proven, inarguable fact based on court records, FISA data, IT evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

3. Your financial office is aware of these facts and has chosen not to replace all of the at-risk equipment, nor sue the manufacturers who sold your organization this at risk equipment. They believe that the hassle and cost of replacement and litigation is more effort than the finance department is willing to undertake. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

4. In addition to the existing tools that were on the internet, in recent years, foreign hackers have released all of the key hacking software that the CIA, DIA and NSA built to hack into any device. These software tools have already been used hundreds of times. Now the entire world has access to these tools which are freely and openly posted across the web. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

5. The computers, servers, routers, cell phones, IP cameras, IP microphones, Smart Meters, Tesla's, "Smart Devices:", *etc.* and other devices openly broadcast their IP data and availability on the internet. In other words, many of your device broadcast a "HERE I AM" signal that can be pinged, scanned, spidered, swept or, otherwise, seen, like a signal-in-the-dark from anywhere on Earth and from satellites overhead. Your devices announce that they are available to be hacked, to hackers. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence

and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

6. It is bad policy for your organization, or any organization, to think they are immune or have IT departments that can stop these hacks. NASA, The CIA, The White House, EQUIFAX, The Department of Energy, Target, Walmart, American Express, *etc.* have been hacked hundreds of times. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

7. The thinking: “Well, nobody would want to hack us”, or “We are not important enough to get hacked” is the most erroneous and negligent thinking one could have in the world today. Chinese, Russian and Iranian spy agencies have a global “Facebook for blackmail” and have been sucking up the data of every entity on Earth for over a decade. If the network was open, they have the data and are always looking for more. The same applies to Google and Facebook who have based their entire business around domestic spying and data re-sale. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

8. You are a “Stepping Stone” doorway to other networks and data for targeted individuals and other entities. Your networks provide routes into other people’s networks. The largest political industry today is called “Doxing” and “Character Assassination”. Billions of dollars are expended by companies such as IN-Q-Tel -

(DNC); Gawker Media - (DNC); Jalopnik - (DNC); Gizmodo Media - (DNC); K2 Intelligence - (DNC); WikiStrat - (DNC); Podesta Group - (DNC); Fusion GPS - (DNC/GOP); Google - (DNC); YouTube - (DNC); Alphabet - (DNC); Facebook - (DNC); Twitter - (DNC); Think Progress - (DNC); Media Matters - (DNC); Black Cube - (DNC); Mossad - (DNC); Correct The Record - (DNC); Sand Line - (DNC/GOP); Blackwater - (DNC/GOP); Stratfor - (DNC/GOP); ShareBlue - (DNC); Wikileaks (DNC/GOP); Cambridge Analytica - (DNC/GOP); Sid Blumenthal- (DNC); David Brock - (DNC); PR Firm Sunshine Sachs (DNC); Covington and Burling - (DNC), Buzzfeed - (DNC) Perkins Coie - (DNC); Wilson Sonsini - (DNC) and hundreds of others to harm others that they perceive as political, personal or competitive threats. Do not under-estimate your unintended role in helping to harm others. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

9. NEVER believe that you are too small to be noticed by hackers. Parties who believe that are the hackers favorite targets. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

10. NEVER believe that because the word “DELL” or “IBM” or “CISCO” is imprinted on the plastic cover of some equipment that you are safe. Big brands are targeted by every spy agency on Earth and are the MOST compromised types of equipment. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented

evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

11. YOU may not personally care about getting exposed but the person, or agency, you allow to get exposed will be affected for the rest of their lives and they will care very much and could sue you for destroying them via negligence. Be considerate of others in your “internet behavior”. Do not put anything that could hurt another on any network, ever. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

12. Never post your real photograph online, or on a dating site social media or on any network. There are thousands of groups who scan every photo on the web and cross check those photos in their massive databases to reveal your personal information via every other location your photo is posted. These “image harvesters” can find out where you, who your friends and enemies are and where your kids are in minutes using comparative image data that they have automated and operating around the clock. This is a proven, inarguable fact based on court records, FISA data, IT evidence, national news broadcasts, Congressional presented evidence and inventory records, ie: Krebs On Security, FireEye, ICIJ, Wikileaks Vault 9, EU, Global IT services, FBI.

13. If you think using web security measures like this makes you “paranoid”, then think again. Cautious and intelligent people use these security measures because these dangers are proven in the news headlines daily. Uninformed, naive and low IQ people

are the types of people who do not use good web hygiene and who suffer because they are not cautious and are not willing to consider the consequences of their failure to read the news and stay informed.

- Provided By The Broadcast News Association - 2019

MORE PROOF:

https://www.i-programmer.info/news/149-security/12556-google-says-spectre-and-meltdown-are-too-difficult-to-fix.html

https://sputniknews.com/us/201902231072681117-encryption-keys-dark-overlord-911-hack/

https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2

https://thehill.com/policy/technology/430779-google-says-hidden-microphone-was-never-intended-to-be-a-secret

https://www.blacklistednews.com/article/71200/smartphone-apps-sending-intensely-personal-information-to-facebook—whether-or-not-you-have-an.html

https://www.bleepingcomputer.com/news/security/microsoft-edge-secret-whitelist-allows-facebook-to-autorun-flash/

https://news.ycombinator.com/item?id=19210727

https://www.davidicke.com/article/469484/israel-hardware-backdoored-everything

https://www.scmp.com/economy/china-economy/article/2186606/chinas-social-credit-system-shows-its-teeth-banning-millions

https://youtu.be/lwoyesA-vlM

https://www.zdnet.com/article/critical-vulnerabilities-uncovered-in-popular-password-managers/

https://files.catbox.moe/jopll0.pdf

https://files.catbox.moe/ugqngv.pdf

https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

https://arstechnica.com/tech-policy/2019/02/att-t-mobile-sprint-reportedly-broke-us-law-by-selling-911-location-data/

https://theintercept.com/2019/02/08/jeff-bezos-protests-the-invasion-of-his-privacy-as-amazon-builds-a-sprawling-surveillance-state-for-everyone-else/

https://www.blacklistednews.com/article/71200/smartphone-apps-sending-intensely-personal-information-to-facebook—whether-or-not-you-have-an.html

https://www.stripes.com/news/us/feds-share-watch-list-with-1-400-private-groups-1.569308

https://voat.co/v/news/3053329

https://www.zdnet.com/article/all-intel-chips-open-to-new-spoiler-non-spectre-attack-dont-expect-a-quick-fix/

https://voat.co/v/technology/3075724

https://www.theregister.co.uk/2019/02/26/malware_ibm_powershell/

https://fossbytes.com/facebook-lets-anyone-view-your-profile-using-your-phone-number/

https://www.iottechtrends.com/vulnerability-ring-doorbell-fixed/

https://voat.co/v/technology/3077896

https://www.mintpressnews.com/whistleblowers-say-nsa-still-spies-american-phones-hidden-program/256208/