How to be cyber-safe.

Maximize your security level – protect yourself <u>and</u> clients too!

We all know that large companies like Sony and countless small businesses have been attacked and/or had a data breach. Everyone is a potential target for hackers and their cyber malfeasance. So how do you protect yourself and become "cyber-safe" and can that even be adequately done? YES, to a substantial degree! Doing the below steps will help you be maximally prepared, so when the bad guys scan the internet your PC won't be easily found or be that "low hanging *hacker* fruit." Most attackers like easy targets; these steps make it much harder to steal your data.

We use several existing security guides with very useful information; these current best practices help you build a known baseline. It's important to use only approved products ("**NIAP**") and never start anything in cyber from scratch, as someone has already done all the hard work. These guides, methods and products work well because *cyber is essentially 95% the same everywhere!* These are your security best practices and also apply to remote office workers, small office / home office (SOHO) and small/medium business (SMB) - as cyber safe is universal!

This cyber safe guide has two parts; a short, 'just the facts" key takeaways part for those who want a quick look, bulleted list, and then we map out the key reference materials and detailed rationale and recommendations to use.

Key Cyber Safe Takeaways:

1 – Use *decent passwords* (use a pass phrase to construct it). *Don't use the same passwords on other accounts* (as once they hack one account, your others will fall too).
2 – *Encrypt* your data! (note, we suggest free sources below). *And store your data off-site*, in the cloud or other physically separate place – as when your hard drive crashes or you suffer a ransomware attack, your data is safe.
3 – Always *use TWO computers at home* = (1) general use (kids / web browse, etc) and (2) work / financial. Protect #2 with tight security controls and don't web surf – do business only – thus much less likely to be hacked.
4 – *Use the free security tools* your ISP / cable provider offers, then add the several other free tools listed below.
5 – Your mobile phone is an extension of your office – and most likely a very easy threat vector to hack and get into your accounts. *Follow the suggested mobile security guides* and best practices (re: the links below).
6 – *Wireless* – select strong encryption, disable SSID and change the default password. *FREE wireless - generally assume it's unsecure* (FYI - in southern San Diego over half the access points are owned by one Mexican criminal). Generally b*est to never use 'free Wi-Fi sites'* to be on the safe side, even as when using VPNs, etc. the risk is lower.

Cyber Safe Suggestions and Reference Material

Now on to the detailed suggestions. While we provide a LOT of recommendations, the best way to use this guide is while reading, just jot down or *highlight what you need to do* = your tailor made personal security plan!

1 - This is great list of **<u>overall precautions and security/privacy good habits</u>** for personal and business protections! They offer 15 or so common sense ways to be cyber safe – and go beyond just the PC security we cover below. *''AS You ARE going to get hacked!''* (…if not already)(…well at least your data will be)
https://www.linkedin.com/today/post/article/20140926230113-113107450-you-are-going-to-get-hacked

2 – You must <u>have a **security policy**</u> – yes, you need a simple policy even at home – for the kids, family, anyone using those PC/internet resources (for those of you who did a 'driving contract' with your kids – same principle applies here). Remote employees, SOHO, small and medium business (SMB), etc must have a security policy to feed cyber safe practices (of course so does everyone else) – as policy drives requirements and processes. As we said, always leverage good practices! The State of Delaware has almost *every policy a business needs*!!!
https://dti.delaware.gov/information/standards-policies.shtml
The SANS (a major security group) has many policy examples, they more specifically cover cyber security.
http://www.sans.org/security-resources/policies/

3 – **Individuals, remote workers, SOHO and SMB cyber safe set-up guide**! (e.g., these steps A – M)
A - It does not cost a lot of time or resources for anyone to be relatively well protected. To start with there are several good overall guidance articles to follow – skim them to *see the overall cyber security guidance / key steps*:
https://www.sba.gov/blogs/**9-cyber-security-tips-small-business-owners**
http://www.zdnet.com/article/**10-security-best-practice-guidelines**-for-businesses/
These two links have several other suggestions to configure your PC / SOHO / SMB clients.
https://www.dhs.gov/sites/default/files/publications/**FCC**%20**Cybersecurity**%20**Planning**%20**Guide**_1.pdf
http://windowsitpro.com/networking/**8-steps-secure-soho**

B – **Passwords** – they are still quite useful – *especially "IF" well-constructed* (and you don't need to change them a lot either, if strong). You have heard that the best method is to use a "pass phrase" (some short catchy few words that only you know). Then use the first letter of words, with numbers and symbols in-between, start and end. These are easy to follow rules -- https://blogs.mcafee.com/consumer/15-tips-to-better-password-security

C – **Encrypt!** This may seem obvious, but very few folks actually DO it in practice. FYI - the California Attorney General's *# 1 privacy recommendation*? ***Encrypt***, *encrypt*, encrypt = protects your data, minimizes liability too!

See the *security suggestions from the 2014 mega breaches*. Top ten actions to DO! Privacy lost, is gone forever!
http://www.itbusinessedge.com/slideshows/security-lessons-learned-from-2014-the-year-of-the-mega-breaches.html?utm_medium=email&utm_campaign=ITBE_NL_DYE_20150206_STR1L2&dni=215002847&rni=215180089
Also, Ponemon Institute released their second annual *study on corporate data breach preparedness – so DO IT!*
http://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

So, what are some of the better free / low cost encryption tools?
Use OS tools: *Bitlocker & FileVault*. Or free tools: *Open GPG, AcCrypt*, or from these sites– *just pick one & use it!*
http://www.gfi.com/blog/the-top-2**4-free-tools-for-data-encryptio**n/
http://listoffreeware.com/list-best-**free-file-encryption-softwar**e/

Do you have a *"cyber go bag*" – e.g., scanned all your key / personal documents and uploaded into your cloud?

D – USE your **ISP / Cable firewall** and the one in your home router too. First change the password – do not leave it as the default. (and as we'll suggest later, use the other security tools your ISP provides for free too). There are free firewalls you can use as well. Just pick one and USE it! (*Caveat – not all cyber programs interact well.*)
http://www.pcmag.com/article2/0,2817,2422144,00.asp

BTW… IF you have an older router at home, OR need more BW (who doesn't?) Check out this *ASUS RT-AC68U gigabit wireless* router with firewall ($179 at Amazon). While a consumer level product – it has *extensive built in firewall / malware protection*. Where even if you *get a* "*bot" behind the network, it prevents outgoing connections to command and control nodes! Get this feature in your router!* http://www.asus.com/support/FAQ/1008719/

E – **Computer protection** – start by **using** ***a cyber security suite*.** For example, MS essentials is good (built into later windows OS). Again, always use the FREE cyber suite your ISP / cable company provides. For the most part the key action here is to just turn on and configure the one that come with the OS and ISP!
*BTW, a quick scan for best cyber suite brings up this list (*where in this case "BitDefender" was rated No 1.)
http://internet-security-suite-review.toptenreviews.com/**small-business-internet-securit**y/
Regardless if you use your home computer for work, it's also your computer / DATA; thus buy a decent cyber suite for your home PC, as they are inexpensive and also use the free security tools listed herein for home use.

I recently tried this malware detection program. For me, *it finds quite a lot of malware* for $40, where it seems to find more items than others. (btw, the scanner is free, but does not remove files - try that first, see if it beats yours)
http://finance.yahoo.com/news/**spyhunter**-voted-best-antivirus-anti-153400129.html

F - ALSO use a **separate anti-virus host / PC suite** - *two FREE* anti-virus suites are SOHOS & AVG.
https://secure2.**sophos**.com/en-us/Pages/DownloadRedirect.aspx?downloadKey=e793e22e-34d9-4fac-9f8d-f7a6371ae802
http://download.cnet.com/**AVG-AntiVirus-Free-2015**/3001-2239_4-10320142.html?hlndr=1&part=dl-avg_free_us
NOTE –keep selecting the FREE version, as they try to have you select the 'free trial' version of the paid product. The free version contains the same signature base for virus detection, so you're only adding bells and whistles.

G – A couple of other well-known *free assessment tools* are: "**CCcleaner**" and "**Ad-aware**"
https://www.piriform.com/**ccleaner**/download/standard
http://www.lavasoft.com/download/**adaware**_download.php?lang=en&inter=3875_1009709_digitalrivercomparativelp_null_null_null&src=free_install

H – Set up your **browsers for maximum protection**….
--- *Firefox* – tighten the browser controls to the max… so web sites can't capture your info - and use this browser as your main one, unless it won't work on a site.
https://support.mozilla.org/en-US/products/**firefox/privacy-and-security**

--- *Chrome* – you can lighten up on the security controls here a bit so you can get it to work on more sites.
https://support.google.com/**chrome**/answer/114836?hl=en

--- *Overall browser security setting* support / guidance for all three
https://www.veracode.com/blog/2013/03/browser-security-settings-for-c**hrome-firefox-and-internet-explore**r

--- *SOHO / SMBs must go further* to **minimize the browser threat vector**! We know the browser is "THE" malware threat vector entry point - upwards of 80% of malware comes through it. Where of course all those files are downloaded using HTTPS; so files are encrypted right to the end device - bypassing the cyber suite..;-((
These are a few recommendations to greatly reduce the browser threat space in your SMB / SOHO!
Tighten up your browser controls - especially limit active code (JAVA, Active-X, etc). As recommended above, disable most tracking functions, put the browser into "guest" mode (or equivalent) and force all files to the same user download directory to be automatically scanned.
Then use 'white listing' for both applications (require certs to run) and URL / web sites (this greatly minimizes access to infected IP addresses and most phishing vectors too) http://en.wikipedia.org/wiki/**Whitelist**
And then disable executables from being installed on end devices by users (e.g., require privileged / SysAdmin rights to add software), this makes sure any files put on end devices cannot load / execute (aka, malware / rootkits).
AND for the ultimate in browser and web-site protection, have your webmaster apply the "*OWASP top ten" fixes*!
DO these steps and you have greatly minimized the impact / risks of the browser threat vector!

I – **Mobile phone security.**
This is a HUGE threat vector area all by itself, *for now – just skim and use these guides*.
http://media.gswi.westcon.com/media/Westcon%20south%20africa/newsletter%20images/August2013/21-**BYOD-Dummies**.pdf
http://www.esd-download.com/files/soft/KISAD/EN/kms10_an_userguide_en.pdf
ftp://ftp.symantec.com/public/english_us_canada/products/norton_**mobile_sec_suite**/5.0/manuals/nms_suite_5.0_ug.pdf
Android
http://www.verizonwireless.com/mobile-living/network-and-plans/android-security-app-tips-to-keep-your-smartphone-secure/
http://www.tomsguide.com/us/best-antivirus,review-2588-7.html
http://searchsecurity.techtarget.com/tip/Android-security-settings-and-controls-for-Android-enterprise-security
IPhone
http://www.mcafee.com/us/resources/white-papers/foundstone/wp-top-10-iphone-security-tips.pdf
http://www.tomsguide.com/us/mobile-security-guide,review-1918-3.html
http://www.apple.com/business/docs/iOS_Security_Guide.pdf
BTW - The Calif State Attorney produced this superb 'security' document – on *mobile privacy* - more great "safe" steps!
http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/**privacy_on_the_go**.pdf

J – Wireless – Typically supplied by your ISP, router or separate device – Always select the strongest encryption (WPA2), disable SSID, and use a strong password. As for *free wireless – generally assume it's unsecure*. Best to not use them to be on the safe side, even as with VPNs, etc the risk is lower. Essentially hackers set up shop in SBX & airports with fake access points that transmit *they* are the free wireless point. So once you log on, they have your passwords, etc. You can review the dangers here: http://safeandsavvy.f-secure.com/2014/09/29/danger-of-public-wifi/
There are several good set-up guides / support that are relatively easy to use:
http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm
http://lifehacker.com/the-most-important-security-settings-to-change-on-your-1573958554

K – *So how do you KNOW what your security posture / baseline actually is*? **As knowing your security baseline is really JOB ONE for your cyber safe approach**. Security posture and impacts can be invisible to most, unless you have the right tools and someone who knows how to read and interpret them correctly (e.g., separate out the false positives from critical vulnerabilities for example). The best, most assured way to know your baseline is to have an independent security expert do a vulnerability scan, using an authoritative reference of what's critical in security (for example, the NIST Cybersecurity Framework and their SMB security publication in item "I below).
--- There are *self-assessments* to use – which *help you be aware of your general security posture at least* - answer the questions as best you can for your 'approximate' cyber status – the holes / vulnerabilities will be quite apparent!
The Cyber Security Evaluation Tool (**CSET**) is from the Department of Homeland Security (DHS)
https://ics-cert.us-cert.gov/Assessments
US-CERT - DHS - Cyber Resilience Review (**CRR**) (this is their self-assessment package)
http://www.us-cert.gov/sites/default/files/c3vp/csc-crr-self-assessment-package.pdf
NIST Security Self-Assessment Guide (based on 800-53)
http://csrc.nist.gov/groups/SMA/fisma/documents/Security-Controls-Assessment-Form_022807.pdf

L – Want to know even more about the cyber big picture and the key capabilities / processes to implement in your SMB / SOHO environment – then *check out these easy to read 2 and 3 page papers* – learn the cyber essentials!
--- *CISO Fundamentals:*
While the SONY and much more aggressive Anthem hacks are causing more folks to be aware of the criticality of cyber protections, instead the typical organization continues to admire the problem / threat (the vast majority of articles just spread scare tactics). So what exactly should we advise folks to DO? We developed a 2-page "*CISO Fundamentals / Cybersecurity essentials*" paper that starts to do just that. An introduction page with the cyber background, where the 2nd page provides a specific dozen or so recommendations for an affordable, effective and "due diligence" set of cyber tenets for folks to embed in their risk management plan and actually implement them.
http://www.sciap.org/blog1/wp-content/uploads/CISO-Fundamentals.pdf

--- *Executing an effective security program:*
For an in-depth set of key security recommendations (distilled from our "CISO Fundamentals" paper), and how to best to execute them, check out our "*Executing an effective security program."* It includes several examples of a 90-100 day timeline - with added recommendations / points on each key cyber tenet – all in 3 pages ("it's in there!"). With these priority tasks, hints and resources, your effective, prioritized, security plan is almost written.
http://www.sciap.org/blog1/wp-content/uploads/Executing-an-effective-security-plan.pdf

M –*Epilog - For an overall small business security approach - skim THIS pub*. As always, NIST has a great pub on **small business security**. Make it a point to read this and "just DO IT" – that is, implement their *absolutely necessary" security steps* – and - for added measure and security also implement their "*highly recommended*" steps.
*** These 20 or so activities gets you *as close to a formal "due diligence" level of security as you can get*!!!
http://csrc.nist.gov/publications/drafts/**nistir7621-r1**/nistir_7621_r1_draft.pdf

To put effective and affordable cyber security and privacy into your personal computing devices and business overall, contact **Mike.Davis.SD@gmail.com** who will connect you with many other SD Cyber SMEs and organizations who offer SMB help!
For more detailed information on many other cyber and privacy resources see: http://www.sciap.org/blog1/?page_id=1184