reddit_microsoft_10_percent.docx

Misleading headlines are misleading (but...)\n\nTL;DR: Use and understand http://haveibeenpowned.com \- maybe even subscribe\n\n\[Sorry wall of text follows\]\n\nThere was no big new breach a month ago. No new data was stolen. Aggregation of past breaches are nothing new. You shouldn't change your password just because a scary news article tells you your details may have been stolen.\n\nThe facts, some but not all made it though the hype filters of the reporters:\n\n* this is a cut and paste list of data from previous breaches, many of them already high-profile, going back several years.\n* Many of those leaks were personally identifiable information (think email addresses and names) - but *not* passwords\n* If your details were included, then they've been known for a time, so don't rush to make changes that might not be the best ones.\n\nThere's some good advice around, though:\n\n**Find out if your data is among the leak leaked**\n\nDon't assume it was, or it wasn't. Try http://haveibeenpowned.com \- it is a well respected service based on aggregating the breaches just like in the headline, but make it searchable by your email address so you can see if you're impacted.\n\n***Never*** **type your password into a site which says it will look it up**\n\nThey only need the email address, never the password. 100% that want the password are either hackers collecting them to sell, or people thinking they're doing something helpful, but making things *much much* worse. Mostly the former.\n\n**Understand what was leaked**\n\nMany of the breaches leak only personal data - likely names, email and physical addresses, etc. In this case you can't do much other than be aware that someone has your information and could try to use it for fraud. If you've been on the internet for more than 2 years or so, you will almost certainly be in this category anyway.\n\n**IF your password is leaked, change it to something strong**\n\nChanging your password is a hassle, and if you're doing it in a panic, you're likely to change it to something insecure.\n\n* t3x7M3554G3 type passwords **are insecure**. If you can see that a E and 3 look similar, so can a computer!\n* Adding or changing a digit ("password17"->"password18") similarly don't delay someone who wants access to your account\n* The [Correct Battery Horse

Staple](https://xkcd.com/936/) method is good, and you can have some fun creating the passwords too!\n* Password managers (LastPass, 1Password, KeePass, etc) will generate - and remember - strong passwords for you. Ask the most tech-savvy person you know for their personal recommendation (and if they don't use one, get better friends!)\n\n**DO NOT use the same password on multiple sites.**\n\nIf I use the same password for gmail, reddit, amazon, linked-in and facebook; and if any one of them leaks it (looking at you linked-in) you have to change passwords in 5 places (more likely 20+ for most people). If you had a different password for each, you'd only ever have to change 1. The misuse of most passwords are in taking a password leaked from a small site (with poor security) and try it on more valuable ones; trying your Webkinz password on email providers and banks.\n\nYes, remembering all these different passwords will be hard, especially if they're good, strong passwords - so again look at password managers.\n\n**Use 2-factor for anything you care about, if you can**\n\nIf the password alone isn't enough to give someone access to your email, credit-card or (worse) reddit karma, then you still have to change it, but your precious upvotes are safe. It's not as annoying as you might think to have to get a code from your phone, or press your laptop's biometric sensor every now and then. There's also recent work to standardize, so you use the same app or fingerprint reader for everything.\n\n**Don't make things difficult for yourself**\n\nIT Departments in the 90's (and those still stuck in the 90's today) enforced policies of making people change their passwords every month (or 2, or...) on the belief that by changing exposed passwords, they'd make things more secure. Research and experience now shows the opposite is true: if you force someone to change their password when they don't want to, they choose bad passwords and measurably decrease security. If you have a good password that you don't think has been leaked, don't change it just for the sake of it.\n\n**If you're not sure, get good advice from someone you trust.**\n\nMany banks and major service providers (Google, Microsoft, Apple, Ebay, ... \[Probably best not to mention Facebook after the Cambridge Analytica scandal ;) \]) have good advice sections on their web site relating to safety online. Government websites too have slowly caught up with best practise. One thing I would recommend against though is just taking the word of some bloke on the internet that turned up in a search, or bubbled onto your reddit

feed.\n\nOh.... erm.....\n\nBe safe - and if you're not sure, find someone you trust to ask....

The government announced that Microsoft was attacked with the world's biggest hack by Chinese hackers. Then the next day Microsoft rallies. What a strange market.

[Reinforce]

[At least we know the security has been tested recently...] (https://www.reuters.com/article/us-usa-cyber-microsoft-idUKKBN2AX23U)

"Anti-Keylogging" software for 19.99. Nah. This is not appealing to retailers. Antivirus/ security software is a saturated market, and Microsoft/apple are doing a better job of providing adequate security services every year, so it is a shrinking market. I doubt the government or big businesses would buy security software from anyone but the big names in the industry. \n\nsource: been in cyber security industry for 12 years; but hey, I'm not a financial advisor, just some rando on the internet you do you.

And the Microsoft hack

Calling it now, ARK got owned by the Microsoft OWA Hack

" **White House national security adviser will identify actor behind Microsoft hack in near future** " \n\nwho yall think? jared leto doing some method acting tryna get in touch with da joker?

New limits on huawei, bullish BB and NOK. If China gets blamed for Microsoft hack, even more bullish. Who wants china spy gear in their critical telecom infrastructure?

Yeah this is most likely true. The used to be a program run by ASD that certified the security of Government run IT Systems. Quiet complex stuff and certainly too big to explain here but to make it simple. One of the controls in place to keep the integrity of data to our systems was that they had to be hosted in Australia and only accessed by Australian people. A

couple of years ago the former Cyber consultant to Malcolm Turnbull wanted to allow Microsoft to host their data here for Australian systems but be managed by people in the US. The Head of the security program blocked it as so she should cause it didn't align with the controls. So what did they do? Put her out to "Garden Leave" and the cyber consultant become Head of the security program. Consequently allowed Microsoft to access systems from the US..not long after Amazon was also allowed.

[New nation-state cyber attacks - release by Microsoft] (https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/)

Also there's this from a Wired article:\n\n"The law would mandate that every new smartphone and tablet sold in the state would come with a preinstalled adult content filter activated by default. This makes no sense on a few levels—logistical, constitutional, ethical—but fortunately also seems to have little chance of any near-term effect; the bill stipulates that its requirements don't go into effect until five other states have passed identical legislation, and even then it seems unlikely that Apple and Google and the Electronic Frontier Foundation and basically anyone within a thousand yards of the intersection of civil liberties and technology would acquiesce to Utah's
demands."\n\nhttps://www.google.com/amp/s/www.wired.com/story/utah-porn-bill-microsoft-exchange-hack-security-news/amp\n\nFortunately it seems the law won't do much, even if it does showcase a lack of concern for anything but the religious values of mormons.

Ok so when people say cybersecurity they are generally thinking Pentest and audit type roles. Teh 3l!t3 Haxxors as it were. Most cyber security is actually just a role It departments fill when they go about their day. Making sure everything is patched. Running port scans to make sure nothing os open that isn't supposed to be. for this role yoou'll generally go the traditional IT route. 4 year degree, mostly Computer science but most STEM degrees will work. maybe a masters in CS or a specialization. Certificates starting with A+, Network+ , Sec+ then a Microsoft cert Which are in flux right now because Microsoft retired the MCSA. So there's an O365 and a Azure cert they are pushing. Then CCNA or Linux+. This will

get you to middling Professional in IT. at this point you'll probably have been sent to a specialty somewhere. Which is really going to depend on your work experience. You might be doing a lot of backup and data protection, you might be doing a lot of cloud stuff and devops. but if you get to a role more in the security risk management, you can start working on your CISSP. \n For the Elite Haxxor route. The one person I know that got there. had a dual major in math and CS. had a decent internship and participated in coding events where you do stuff like build a game over a weekend as well as 0wn this box challenges where you hack into a computer on a network that has had some intentional holes left open. His interview was pretty much it's own 0wn this box where he had a couple of weeks to find all the security holes on a prepared server and write a report to the hiring manager. That stuff isn't going to be taught in school, that's shit you need to pick up in your down time.

The chines were very bullish on Microsoft today. They found a good way to hack office exchange program

We had someone like that at my old work. \n\nWe did PC repair and she swore her ex husband worked for Microsoft in Redmond as part of the windows team. He was therefore trying to hack her all the time, and was successful. \n\nI used to refer to her as “a cat that came to life as a human” because that’s the general looks and vibe she had. Like she was always one step away from completely snapping at whoever was closest. \n\nTurned out her ex husband actually was a senior engineer on the windows team! However there was literally zero evidence he ever did anything to her computer. Someone was finally just like “Why don’t you buy a Mac?” \n\nShe left us alone at that point.

I see a lot of anti-scammer YouTubers. And many of the scammers they show seem to be from India. They pretend to be from the US government and tell people they'll go to jail if they don't send the scammer's money. They will also pretend to be from Microsoft and will hack into people's computers, claiming to fix the computer, and steal their data. \n\nDo you feel that these scammers are ruining India's reputation? \n\nI also see that many people who come to America from India are usually very nice and are often business owners, technology experts, doctors, etc. I feel like many

people from India are smart people, but it makes me sad to see that so many scammers don't care about how they're portraying their country. I don't want people to hate Indians or to think they are all scammers. \n\nDoes the Indian government try to stop these scammers? \n\nIs there something that people can do or say to these scammers when they get called by them, to hopefully stop them from taking advantage of others?\n\nWhat Indian food should be popular all over the world? \n\nAnd finally:\n\nAmericans do Henna tattoos for fun, and also believe in chakras and things like that. Is this bad, and stealing, or is it okay for Americans to do this? \n\nI always thought Henna was pretty but I don't want to steal and appropriate other cultures, especially since I heard it is typically only used in special events like weddings.\n\nI'm sorry for all the questions lol. You don't have to answer them all.

Microsoft was affected by the SW hack. BB was not.

They use Microsoft Exchange, which had a series of vulnerabilities being actively exploited from January onwards. Microsoft have blamed a "Nation state group called hafnium from China for the hack.\n\nHaving said that, by early Feb, the vulns were widely known and the WA hack could have been done by any number of groups, including local script-kiddies *[Disappointment]*.

Frankly the market underestimates the danger that companies whose primary product is software face on a daily basis. Microsoft, Apple, Google, the majority of their IP is digital and as we've repeatedly been reminded, nobody is immune from cyber attacks. Especially as the Cold War with China heats up, the risk increases exponentially. Is it crazy to imagine China someday hacking Apple as retaliation for the US crippling Huawei?

Depends on how you want to define "cybersecurity" then\n\n\n\n* Red team exercises where subject matter experts look for threats within your company, and try to address them\n* Information security agents within a company who organize bug bounties, paying crackers (and not hackers, plz) for information\n* Network providers who defend against DDoS attacks or packet inspection\n* Software development teams who work with the life cycle products to scan the CVE vulnerability databases and see what matches within a

company\n* AI type of teams which look internally at software development and network traffic for unusual patterns\n* Etc.\n\nCyber security isn't young, it's been around for years ever since we worked with RFC and understood that "daemon" as a username / password wasn't appropriate for UUCP. Understand what area you want to examine or think is a growth is key. \n\nE.g. Microsoft picked up GitHub, which is the premier open source hosting location. This gave Microsoft tons of insight into the software development workflow of individuals, teams and companies. Along with data analysis. Subsequently, GitHub acquired Semle which is using CodeQL and variants for analyzing software (instead of of just searching for a string). \n\nE.g. Palo Alto Networks (firewall products) have been doing packet inspection for ages\n\nE.g. Splunk has been doing the log forwarding for a while, even buying real estate in San Jose to expand\n\nE.g. Cloudflare which assist companies in fending off DDoS\n\nPoint is that there is no one company, team or product which meets all of the needs or demands of cybersecurity these days.

This is the best tl;dr I could make, [original] (https://apnews.com/article/beijing-china-email-870dfcc0b3dc9a95a641a85081464018) reduced by 90%. (I'm a bot)\n*****\n> RESTON, Va. - Cyber sleuths have already blamed China for a hack that exposed tens of thousands of servers running Microsoft's Exchange email program to potential hacks.\n\n> Mandia said his company assesses based on the forensics that two groups of Chinese state-backed hackers - in an explosion of automated seeding - installed backdoors known as "Web shells" on an as-yet undetermined number of systems.\n\n> Mandia compared the Exchange hack with the SolarWinds hacking campaign that Washington has blamed on elite Russian intelligence agents that his company discovered in December.\n\n\n*****\n[**Extended Summary**] (http://np.reddit.com/r/autotldr/comments/m2400v/fireeye_ceo_reckless_microsoft_hack_unusual_for/) | [FAQ] (http://np.reddit.com/r/autotldr/comments/31b9fm/faq_autotldr_bot/ "Version 2.02, ~563154 tl;drs so far.") | [Feedback] (http://np.reddit.com/message/compose?to=%23autotldr "PM's and comments are monitored, constructive feedback is welcome.") | *Top*

keywords: **hack**^#1 **Mandia**^#2 **China**^#3 **Chinese**^#4 **wave**^#5

If I understand you correctly, yes, I think so. Let me explain.\n\nCMMC Level 3 contains all of NIST 800-171 in its entirety. It also contains an additional 20 requirements that are new and unique to CMMC. \n\nAchieving CMMC while using a cloud provider will depend on the cloud provider **agreeing to take the flow-down of your cyber security requirements**. In other words, because your company has a contract with the DoD, you have to fulfill these cyber requirements AND you are required to pass those requirements onto your subcontractors and IT partners. To pass a CMMC audit, you'll (probably) need some kind of documentation or signed contract with your IT provider stating that they comply with CMMC and that they accept the contractual flow-down of *your* security requirements.\n\nBy the way, this is the main reason why a lot of people use Microsoft GCC High. Microsoft makes it very clear that they will accept flow down of NIST 800-171 from its customers.

The Shadow Brokers is a hacker group. It carried its first hacking attack in August 2016. It has carried out 5 major cyber information leaks. The following leaks were done on October 31, 2016, April 8, 2017, April 14, 2017, and May 2017. \n\nThis group published several unredacted documents containing hacking tools. Reports say that these documents were hacked from "Equation Group", which is believed to be US National Security Agency’s (NSA) branch. The documents leaked were mostly related to the Tailored Access Operations unit of NSA. \n\nThe exploits and vulnerabilities mainly targeted Microsoft products, antivirus software, and enterprise firewalls. \n\nYour question particularly mentions the WannaCry ransomware attack by this hacker group, Shadow Brokers. This attack was the group’s most infamous and destructive attacks. It used the ETERNALBLUE exploit on Server Message Block (SMB) for spreading itself. This attack infected more than 200,000 machines within the first 2-weeks. \n\nETERNALBLUE contains kernel shellcode for loading the non-persistent DoublePulsar backdoor, allowing installation of the PEDDLECHEAP payload that gives the attackers access by using the DanderSpritz Listening Post (LP) software. \n\n*“The New York Times put the incident in the context of the Democratic National Committee cyber

attacks and hacking of the Podesta emails."*\n\nGiving a view on this matter will definitely is out of my domain knowledge As it is not related to my financial domain knowledge. However, I can only say that the Shadow Brokers' leaks are different from those done by Snowden's Wikileaks. While Snowden followed the journalistic care by redacting too sensitive materials, the Shadow Brokers leaked all the materials unredacted.\n\nThe most interesting thing in these leaks is that the attackers kept those hacked documents to themselves for 3-years and released them only after that. This is very uncommon in case of Whistleblowers. \n\nMany believe that the attack was carried out by a nation-state, probably anyone from Russia, North Korea, Iran, China, Israel, or any other country. As said by David Aitel (a computer scientist formerly employed by the NSA):\n\n*"I don't know if anybody knows other than the Russians. And we don't even know if it's the Russians. We don't know at this point; anything could be true."*\n\nBy the way, if you are interested in cryptocurrency trading and want to create a passive income stream through crypto investment like a pro, you may try [NapBots.com](http://napbotscom.space/). It is an advanced copy-trading AI bot that scans the market in real-time and automatically trades for you (when put on autopilot). \n\nYou can exploit their 15 years of experience in quantitative trading at global financial institutions. If you don't have the time to study charts and graphs, let the experts trade for you, and copy exactly what they do. \n\nYou don't have to monitor charts and candles to predict your next move. Any novice trader with zero skills can also start trading like a pro and earn money with this unique trading tool. They run 24/7, which means that you can keep earning your passive income even when you are sleeping. This gives you an edge over other investors as it enables the bot to book profits on your behalf when other investors are sleeping.

Use windows defender and comment sence. Microsoft is one the best cyber security companies out there and the best defense you have is commen sence

Once you have deactivated everything. I would add that you create a new email and notify all of your contacts of the issue. Ask them to block old email and ignore anything from it. And to contact you from now on via new email. Add that they can call you if they are unsure to verify it is you in

person. Start with work related first, then personal. I know mortifying but job is more important. Then go over if you can and help older relatives to block and save new email. And also help them do software updates on their devices and malware scans. This last part is just as important. Why? \n\nMicrosoft earlier in the week announced a data breach due to an exploit hackers took advantage of. They have been able to acquire personal information from many individuals and businesses. It was discovered months ago and a fix has been put into updates. Part of the announcement specifically stated that users may still be vulnerable due to the number of computers that still have not updated. *[Worry]* And / or the hackers could have installed back doors to maintain access, this is why a scan for malware is also important. It may very well not have been your fault, so don't beat yourself up too much. Large companies having data breaches is becoming more frequent. *[Disappointment]* They suspect the hack is by a group of hackers tied to the government of China. Scan your computers, and update today!\n\nhttps://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/\n\nhttps://www.bloomberg.com/news/articles/2021-03-12/hackers-rushed-in-as-microsoft-raced-to-avert-mass-cyber-attack\n\nRead the above news articles for more information. As I recently had a scammer incident as well. They were unsuccessful, but they had a surprising amount of my personal data. I am adding the following fail safes in addition to the above suggestions. I am changing all of my automatic debits for streaming services to a credit card not tied to my bank. If you do not have one, go get a prepaid visa from the local store. I am also only going to use this card for online shopping as well. I set the card up to notify me for every purchase. From now on anytime I use a card on the web it will be only this one. And I get an instant text when it is used, so no surprises. \n\nI hope this helps you to prevent any damage from the hackers now and in the future. And I hope it prevents anyone else from experiencing the same issue

I sure hope they do, it sounds like Biden's NSC is looking into what would be good software security standards after the Microsoft hack which is a start.

Wonder if its also linked to Solarwinds as I saw an article saying MS Exchange source code was obtained in that hack. [https://www.zdnet.com/article/microsoft-says-solarwinds-hackers-downloaded-some-azure-exchange-and-intune-source-code/] (https://www.zdnet.com/article/microsoft-says-solarwinds-hackers-downloaded-some-azure-exchange-and-intune-source-code/)

I study computer engineering and everybody has windows installed on their laptops (there are no macs down here) because of the same reason you mentioned before: this partnership between unis and microsoft. When they see you rocking linux they think you are some kind of freak, that linux is just for servers or that you're going to hack into the matrix or something. I just enjoy the open-minded experience, the freedom and the fact that there are other things besides windows. Sometimes way better.\n\nThe funny thing: the Director of Civil Engineering uses opensuse with kde on his notebook lol

That would make too much sense for Microsoft.\n\nIt is a hassle and if your internet is fast then fair enough. The only time you'd really need to be in the registry though is to find out what game the big files are for as googling for "F5A6AB7C-E2AC-467D-B689-68F29D795DE3" only turns up some Chinese site but the registry will tell you that's actually Yakuza 0. Would be nice if there was a master list somewhere but I'm lazy (and I'd have to install every game on game pass to find out!). \n\nI use a "registry hack" to [add take ownership to the context menu] (https://www.howtogeek.com/howto/windows-vista/add-take-ownership-to-explorer-right-click-menu-in-vista/) which saves you mucking about in the registry for that. You'd then just take ownership of the whole WindowsApps folder and rename it to whatever.\n\nStart downloading one of the games and pause it. Move the corresponding file from the old folder in the new MSIXVC folder (which you'll probably have to take ownership of too). Unpause the download and it'll instantly complete.

I did some further research on this (I am evaluating the app for a relative). What I have notice is that the app has a flaw in regards to recovery. Here's the steps\n\n1. Install MS authenticator on a phone. \n2. You select recovery option, which prompts you to login. \n3. You login and select the option to

send a recovery code by email. \n4. You log into the the recovery email and then enter the code. The 2fa vault is populated.\n\nThe problem here is that all you need to do is hack into the recovery email. You can protect the recovery email with another 2FA, but I feel like it's not a self-contain solution. \n\nMicrosoft could make this safer if they add a master password or passcode to the vault, so that if the user managed to hack the recovery email, they can't get to the vault without the password or limit devices. In fact, since I notice that they are trying to turn MS authenticator into a password manager, they should definitely do that.\n\nAnother change they could made to white list devices or block new devices to prevent people from adding devices. \n\nBoth of these features of block devices and master passcode seems to indicate that the designer of Authy had though hard about security parts. One other factor is that Authy actually published good documentation on how their system work and how they store and encrypt their seeds and how encryption is end to end. Microsoft is not so clear on the matter, they don't say if they encrypt their seed or if it's end to end. I would think security expert may have some issue recommending things they don't have info on.\n\nWhile this may seem like I am some sort of Authy evangelist, I am not. I don't like that the App uses SMS to install and do not use the App. However, good features and policies are good features and policies regardless of the app. \n\nI think I am going to steer my relative towards Authy to see if that would be acceptable.

I had some further thoughts about this. I am not liking the recovery method used for Microsoft Authenticator. Because it uses a Microsoft Account, Microsoft account must have a SMS or email recovery. The SMS would be a bad idea, so email is lesser of 2 evil. The problem is now all they need to do is hack into the recovery email account. One could protected it with something like a hardware key, but it's kinda of stupid to use another 2fa to protect your 2fa. They could make this more secure by adding a master password to the 2fa vault. That way if they hack your recovery account, they would still need the master password to get in.\n\nAuthy does this a bit better. Not because it uses SMS, but because the vault is protected by a password and you can restrict adding additional devices.

>Microsoft revealed the extent of the hack in a blog post Tuesday, saying a consortium called Hafnium used virtual servers in the U.S. to carry

out a coordinated attack in an effort to lift secrets of all kinds pertinent to various different sectors. Cybersecurity firm Volexity said it detected unusual activity deriving from Microsoft Exchange Server programs in January and found the operation based in China. In 2009, a Congressional advisory group told federal lawmakers that China's espionage efforts were "the single greatest risk to the security of American technologies. *[Worry]*"

Outlook is Microsoft. And it was part of the exploit. Link to 2 of the articles in my earlier comments. And I have found a recent Apple data breach in December 2020. I don't use Apple computers so I don't know more specifics. I only know that recent updates corrected exploits they used for that hack.