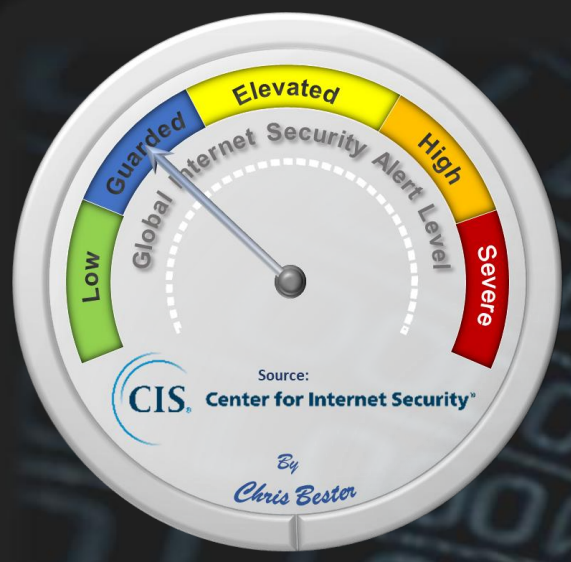


On March 3, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Google and Microsoft products.

Covid-19 Global Stats

Date	Confirmed Cases	Deaths
05-Mar	116,216,656	2,581,649

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

05 March 2021

In The News This Week

More Details Emerge on the Microsoft Exchange Server Attacks

The attacks seem more widespread than initially reported, researchers say, and a look at why the Microsoft Exchange Server zero-days patched this week are so dangerous.
Security researchers believe attacks exploiting four critical Microsoft Exchange Server vulnerabilities extend beyond the "limited and targeted" incidents reported by Microsoft this week when it issued patches for the zero-day flaws and urged enterprises to patch immediately. Organizations first learned of the Exchange server zero-days on Tuesday when Microsoft released the fixes. It attributes the activity to a group called Hafnium "with high confidence." Hafnium is believed to operate out of China and primarily targets organizations based in the United States, Microsoft reports. As more security researchers track the activity, new details emerge about these active exploits, how they were found, and factors that drove the release of this week's out-of-band patches….
Read the full story by Kelly Sheridan here: DarkReading

Cybersecurity firm Qualys is the latest victim of Accellion hacks

Cybersecurity firm Qualys is likely the latest victim to have suffered a data breach after a zero-day vulnerability in their Accellion FTA server was exploited to steal hosted files. In December, a wave of attacks targeted the Accellion FTA file-sharing application using a zero-day vulnerability that allowed attackers to steal files stored on the server. Since then, the Clop ransomware has been extorting these victims by posting the stolen data on their ransomware data leak site. As Accellion FTA devices are standalone servers designed to be outside the security perimeter of a network and accessible to the public, there have been no reported attacks on these devices leading to internal systems compromise. Yesterday, the Clop ransomware gang posted screenshots of files allegedly belonging to the cybersecurity firm Qualys. The leaked data includes purchase orders, invoices, tax documents, and scan reports. . . Read more about it here: Bleeping Computer & Qualys Blog *(Thank you Sergio Stefani for the Qualys link)*

United Kingdom Forms Cyber Security Council

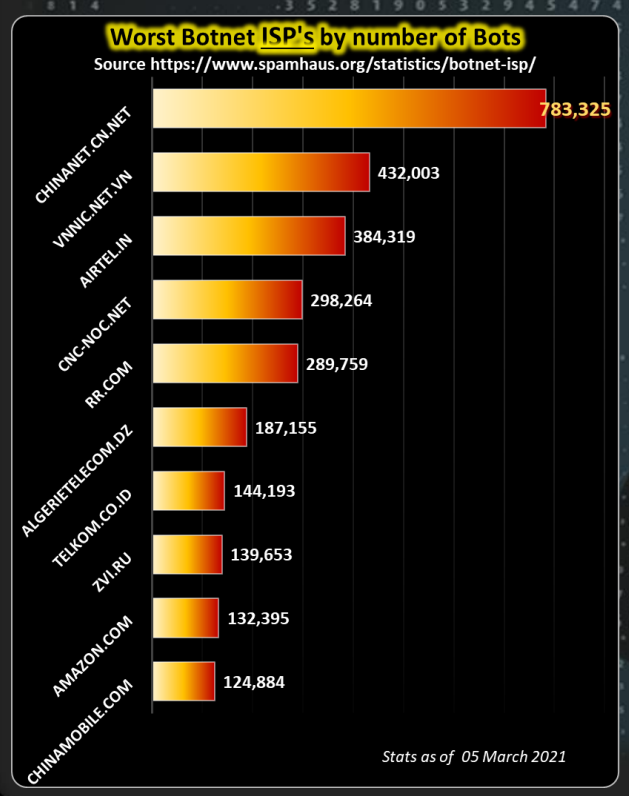
As part of its five-year, £1.9 billion ($2.65 million) national cybersecurity strategy, the UK government on February 9 announced the launch of the UK Cyber Security Council (Council), a new independent body to support career opportunities and set professional standards for the UK's cybersecurity sector. The Council will be formally launched on **March 31, 2021**. In September 2019, the Department for Digital, Culture, Media & Sport (DCMS) commissioned a consortium of cybersecurity organizations known as the Cyber Security Alliance to work on establishing the Council. The Council, which will be funded by DCMS, will set standards for the industry and will work with training providers to offer courses and qualifications to meet those standards.
Read the full article by Morgan Lewis here: JDSupra

Free cybersecurity tool aims to help smaller businesses stay safer online

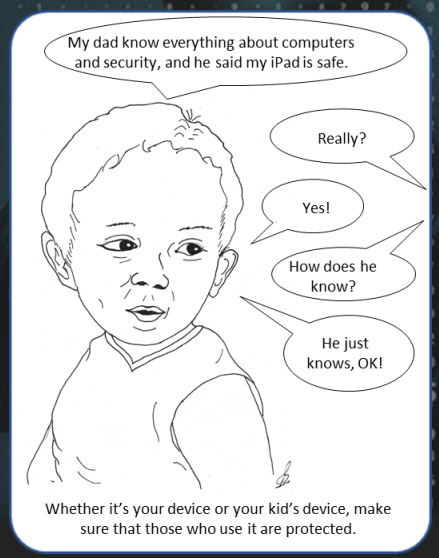
USA - NCSC tool aims to help small businesses develop a strategy to protect themselves from cybercrime. Small businesses can receive bespoke advice on how to improve their cybersecurity and protect their networks from malicious hackers and cybercrime via a new tool from the National Cyber Security Centre (NCSC). The 'Cyber Action Plan' is a free online service designed to help small businesses protect themselves against cyberattacks. While smaller businesses might not believe they're a tempting target for cyber criminals, almost half have reported cybersecurity breaches or attacks over the past year. That figure is up from under a third of SMBs reporting incidents during the previous twelve months. For cyber criminals, while targeting smaller businesses might not be as lucrative as campaigns targeting larger businesses, the potential lack of cybersecurity barriers could provide them with easy pickings. The attacker could always be targeting a small business as part of a supply chain attack against a larger target anyway. Read the full story here: ZDNet

COVID-19 Vaccine Spear-Phishing Attacks Jump 26 Percent

Cybercriminals are using the COVID-19 vaccine to steal Microsoft credentials, infect systems with malware and bilk victims out of hundreds of dollars. Between October and January the average number of COVID-19 vaccine-related spear-phishing attacks grew 26 percent, said Barracuda Networks researchers. At the same time, researchers with Check Point say they have found at least 294 potentially dangerous vaccine-related domains over the last four months. The types of cybercriminal activity varies, from sending malicious emails that purport to be from the Centers for Disease Control and Prevention (CDC), to posting advertisements on underground forums touting vaccine doses for sale. But with the vaccines being rolled out on a widespread basis, these new reports show attackers ramping up their activity on all fronts. Read the full story by Lindsey O'Donnell here: ThreatPost



For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov



Whether it's your device or your kid's device, make sure that those who use it are protected.

How to set parental controls on any phone or tablet

Most parents are deeply concerned about what their kids are exposed to once on the net using a phone, tablet or any web enabled device. It is just not possible to watch over your kid's shoulder all the time to see what they are up to. At the same time you don't want to deny them the privilege of accessing the vast amount of knowledge the modern digital world provides, something that older generations never had. The problem is that you don't want to expose them to the equally vast amount of unwanted content available or intentionally forced down on them. In this light, Popular Science published an updated article this week on how to set up parental controls on the devices they normally use, whether it is yours or their own. Below then is an extract of the article but please visit the Popular Science site to dig a bit deeper.

Tips and apps for peace of mind.

If you've spent any time around youngsters lately, you'll know that they love flat, shiny touchscreens just as much as the rest of us. That means a son, daughter, nephew, or niece will be quick to "borrow" your phone or tablet—or eventually request a device of their own. Whether you're handing your phone to a nagging toddler or sorting out a new tablet for your children, you'll need to protect the device against unwholesome content, unauthorized purchases, and more. Thankfully, it's not that difficult. Here's what you need to do.

Kid-proofing Android phones and tablets

Let's start with a quick fix you can use if a child you're responsible for wants to borrow your phone. It's called App pinning, and it's been part of stock Android since version 5.0. First, head to the **Security menu** in **Settings** and turn the App pinning option On. When you do, a second toggle switch will appear—turn it on. Once App pinning is on, load up the app or game you want to pin, and then swipe up from the bottom of the screen to see the app carousel. Tap the round icon on the top of the preview and choose Pin. To unpin, swipe up from the bottom of the screen again, and your phone will go directly to the lock screen and ask you for your PIN, your pattern, or your pretty face to unlock it.
App pinning is a good temporary fix, but if you want to go for something more comprehensive, you can set up a dedicated user account for a frequent guest. Open System and then go to Advanced. There, choose Multiple users, turn the toggle switch on, and finally, tap Add user. This doesn't add much in the way of parental controls, but it does create a phone-within-a-phone kind of experience, and the new user's apps and settings will be totally separate from yours. To change accounts, drag down from the top of the screen to open the Quick Settings menu, and tap the user icon—it's to the left of the settings' cog wheel. Once there, tap the name of the user you want to switch to.
Android tablets used to have a special "restricted" mode, which allowed parents to control which apps and services their kids could use. This was later replaced (on both tablets and phones) by Family Link, giving parents more capabilities and even allowing them to control their kid's devices remotely. Recently, Google launched Kids Space, a built-in safe mode that, among other functionalities, automatically enables all parental control settings, and only gives access to curated and age-appropriate content on both YouTube and Google Play. The main place to find parental controls on Android, whether for your main user account or one you've set up for your kids, is in the Google Play Store app. Open the main app menu, tap Settings, then Parental controls, and switch them on.
YouTube has its own set of kid-proofing capabilities. Your best bet for child-friendly video-watching is the separate YouTube Kids platform. (See the article for more information on YouTube controls).

Kid-proofing iPhones and iPads

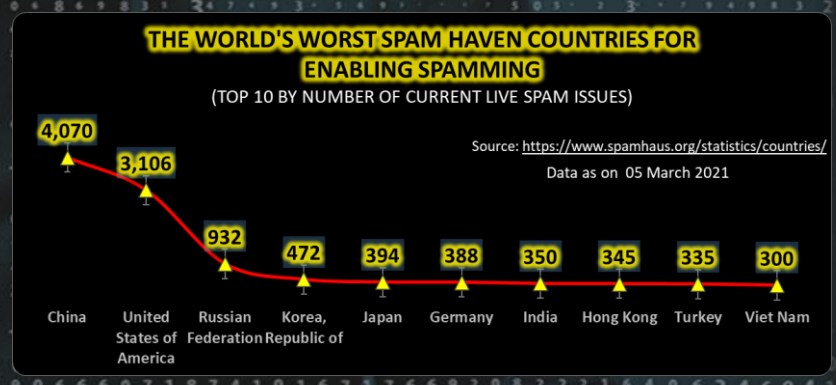
In the land of Apple hardware, kid-proofing devices is fairly straightforward. On iOS and iPadOS, there's a feature called Guided Access, which will prevent your kids from switching to other apps without a PIN code—find it under Accessibility in the Settings app. If you're used to Android, this feature is a lot like app pinning. When you activate Guided Access, be sure to turn on the passcode lock (or biometric protection) and decide how long you want it to sit untouched before the display locks on its own.
Once it's been enabled, you can launch Guided Access for whatever app you or your kids are currently using with a triple-tap on the side button or Home button, depending on your device. At this point, you can also disable certain areas of the screen, lock the volume controls, and even set a time limit for the app. Another triple-tap on the same button will end Guided Access, but your kids won't be able to escape from whatever app you've left them in without your PIN code, fingerprint, or face.
Guided Access works for single apps, whether on your personal device or one specifically for your kids. Elsewhere, the bulk of Apple's parental controls are inside Screen Time. Once you find Screen Time in Settings, go to Content & Privacy Restrictions. Turn the toggle switch on to take control over web browsing, camera use, App Store purchases, and more. Make sure you set up a Screen Time passcode to secure your settings, or else anyone who finds their way in will be able to lift any restrictions you've put in place. The limits you can set here are more comprehensive than they are on Android. It's possible to block access to Siri and FaceTime, prevent apps from being installed or deleted, and build a list of approved websites. Don't worry about having to undo everything when you get your device back either—turn the toggle switch off and it'll deactivate any restrictions or limits you've set up. When it's time to give the device to a child again, turn it on and it'll be kid-safe.

Overall, iOS has better built-in options for putting limits on your kids and Android has a better selection of third-party apps. That said, no matter the make and model of the device you're trying to protect, you should be able to put together something suitable for kids of any age.

See these links and apps for more options & information: MMGuardian, AppLock, Kids Place, Internet Matters, Common Sense

Other Interesting News and Cyber Security bits:

- Gartner 2020 Market Guide for Insider Risk Management Solutions
- Alarming Cybersecurity Stats: What You Need To Know For 2021
- Nottinghamshire schools suspend online learning following cyber attack



AUTHOR: CHRIS BESTER (CISA,CISM)
chris.bester@yahoo.com