Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

The Cyber Threat Alert Level was evaluated on May 12 2021, and was set to Blue (Guarded), and will remain at this level until a change is indicated by CIS.

Covid-19 Global Stats

Date	Confirmed Cases	Total Deaths
02 July	183,416,538	3,971,491

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
02 July 2021

In The News This Week

US, Russia at odds as UN Council confronts threat of cyber attacks

The UN Security Council held its first formal public meeting on cybersecurity, addressing the growing threat of hacks to countries' key infrastructure. The issue was raised recently by US President Joe Biden with Russia's Vladimir Putin. While the US envoy to the world body asked that member states respect a framework already in place, her Russian counterpart called for a new treaty to be drafted. "The risk is clear. Cooperation is essential" to combat such attacks, US ambassador Linda Thomas-Greenfield said, without mentioning Russia, which is often accused by Western countries of hosting hackers or directly engaging in cyberwarfare.
"The framework that UN member states have worked so hard to develop now provides the rules of the road. We have all committed to this framework. Now, it is time to put it into practice." Read the full article here: RTE

South Africa moving 'quickly' to tighten cryptocurrency regulation

South Africa is moving with more urgency to stiffen oversight of cryptocurrency assets after a proliferation of scams. A new regulatory timeline foresees finalising a framework in three to six months, after the publication of proposals earlier in June that require public comment before approval, according to Kuben Naidoo, CEO of South Africa's banking regulator, the Prudential Authority. "We are trying to put in place the regulatory framework quickly," said Naidoo, who's also a deputy governor of the South African Reserve Bank. "Defining this as a financial product and then developing the regulatory framework is important.". The approach that's taking shape means tougher rules could be imminent this year after a jolt of scandals that most recently included a suspected Ponzi scheme, which resulted in the disappearance of an estimated US$3.6-billion in Bitcoin (though the quantum is disputed). South African cryptocurrency service providers have been operating unchecked by regulatory powers even as the popularity of the asset class has taken off. Last year, the collapse of Johannesburg-based Mirror Trading International was called the biggest crypto-related scam of 2020 by blockchain data platform "Chainalysis" Read the full story here: TechCentral

CISA Starts Cataloging Bad Practices in Cybersecurity

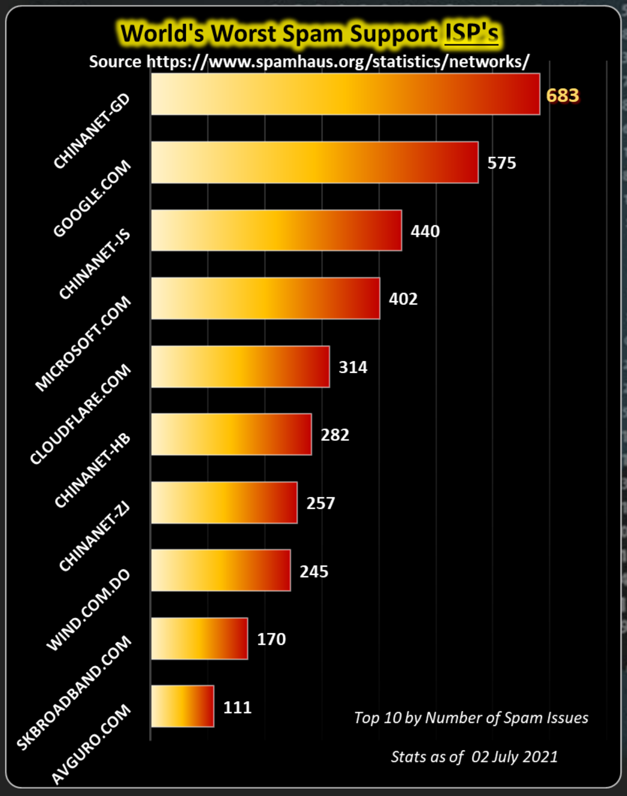
The Cybersecurity and Infrastructure Security Agency released a list of two bad practices Tuesday in an effort to help critical infrastructure providers prioritize their cybersecurity responsibilities. The bad practices are using unsupported or "end-of-life" software, and using known/fixed/default passwords and credentials, according to a blog post published by CISA Executive Assistant Director Eric Goldstein. He said the list is deliberately focused and that the dangerous practices listed are exceptionally egregious in internet-accessible technologies.
"There is certainly no lack of standards, practices, control catalogs, and guidelines available to improve an organization's cybersecurity. While this body of guidance is invaluable, the sheer breadth of recommendations can often be daunting for leaders and risk managers," Goldstein wrote. Read the full article here: NextGov

Putin approves ratification of CIS agreement on cyber security cooperation

Russian President Vladimir Putin signed a bill on ratifying an agreement on cooperation between the Commonwealth of Independent States (CIS) countries in the fight against cyber crimes. The document was published on the official portal of legal information. The agreement was inked in September 2018 at the meeting of the CIS Heads of State Council in Dushanbe, Tajikistan. The document is aimed at establishing modern legal mechanisms for practical interaction of Russian competent authorities with colleagues from other CIS countries for effectively preventing, detecting, thwarting, investigating and solving cyber crimes.
This involves cooperation in the exchange of data on impending or committed crimes and persons behind them, responding to the calls for assistance in providing data that can facilitate the investigation as well as coordinated operations. The agreement defines such terms as malware, data system, unauthorized access to information. The document also establishes that the parties, in line with their national legislation, recognize as criminal offenses the destruction, blocking, modification or copying of data obtained in an unauthorized way, the creation of computer viruses, violation of the rules for using a computer system, if this entailed grave consequences as well as theft by changing the data stored in the system…. Read the full story here: TASS

World's Worst Spam Support ISP's

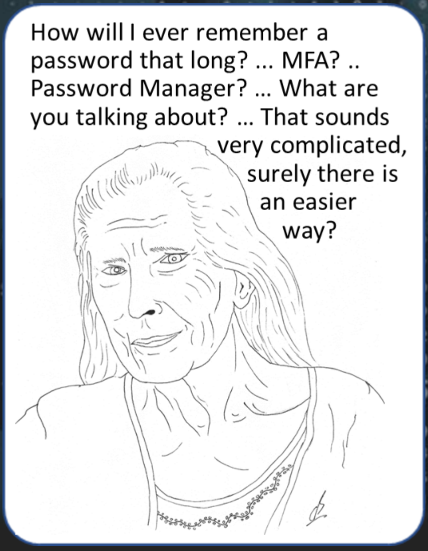
Source https://www.spamhaus.org/statistics/networks/



Top 10 by Number of Spam Issues

Stats as of 02 July 2021

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


How will I ever remember a password that long? … MFA? .. Password Manager? … What are you talking about? … That sounds very complicated, surely there is an easier way?

Cyber Security and the Elderly

We all have elderly family members that find it hard to deal with the modern world of technology that is literally brought to your fingertips. The concept of a wireless thing that can tell you where you are or where to go and can be used to call and even see a friend or family member, are still foreign to them. I can just think of my late mom who grew up in an era where the edge of technology was a handheld flashlight. Or, the fact that you could send a telegram to someone and it actually being delivered in a few days rather that a few months that a letter would take, was really exiting. In the latter part of her life we gave her a mobile phone to call us whenever she needed something, and albeit a very basic model, it was hardly ever used. She preferred using the land line.

The fact is the world is changing and old folks are forced to work with online technology whether they like it or not. Things like online banking scares them but with COVID-19 restrictions, they cannot physically go to the bank and have to go online. Now on top of that, we are telling them about security and how they must protect themselves from people that can steal your stuff from halfway across the world.

The first line of defence is to have a strong password, we tell them. What denotes a strong password they would ask? As all good security guidelines suggest, you will run the password gobbledygook of minimum 13 characters, upper and lower case, numbers, and special characters and so on, by them. We all know that that is the right way but for an elderly person, the first thing that goes through their minds is "how on earth will I remember a password as long as that?" Then you tell them about multifactor authentication where they still have to use their password but also have to do something else as well and you get this blank stare. All this might all sound comical, but for an elderly person it's not. The challenge is, how do we help them to be safe in a simple and manageable way.

What is a good method for elderly people to manage their passwords?

1. Pen and Paper – Now I know this goes against every fibre of a security practitioner's being and is not best practise, but the reality is that the real enemy is the online world. It is highly unlikely that someone will break into someone's home and physically steal their passwords without being noticed. I went through various guidelines and blogs and it is surprising how many actually advise the elderly to do just that. Write down the password and keep it with the rest of your important documents. To remember where you file a piece of paper is substantially easier than remembering a good and strong password.

2. **Password Phrases** - For those who don't want to go down the route of writing down their passwords, or even if you do, you still need to come up with a way of picking a good password. A password phrase is one of the methods that works well as you can build up phrases of things familiar to you without using the standard easy-to-guess family or pet names. One way is to use the picture puzzle method, almost like the online CAPTCHA challenge and response thing. Most folks have pictures or paintings hanging on their walls with some scenery or what-not which they can use. For example if there is a picture of a harbour scene, the password phrase can be something like "3 Boats in the water!". Remember, it is okay to use spaces, and if you throw numbers and capitals in the mix with the odd special character, you will pass most of the password difficulty tests.

3. **Password Manager** – A password manager is commercial online programs or apps that you purchase or subscribe to for a monthly fee. These work great and you only have to remember one password for all your applications. But, if you are an elderly person who already has trouble accessing or understanding these apps, or cannot afford it, then this is not a viable option. Further to this, it is an online service, and in the current world where cyber criminals break into some of the most secure facilities left, right, and center, who knows if the service you subscribe to could be compromised. If you do want to use this method though, make sure you pick a reputable vendor, someone that's been in business for a good while. And if it comes to password manager services, NEVER use a free service!

4. **Two-step Authentication** – Two-step or multifactor authentication is offered by most banks and other financial service organisations nowadays. It is not really something to help you remember your password though but this writing will not be complete if I don't mention it briefly. How it generally works is that you still have to type in your password when doing an online transaction or log on to an app. Then the organisation or app where you want to log on to will either send a one-time-pin or password (OTP) to your phone or ask you to type in the code from an authenticator app that you already have. Without this second code or password, access will be denied or the transaction will be declined. If you do online transactions with your bank and are not presented with this option, please enquire and ask them to enable it, this is an important safeguard.

5. **Gadgets** – if you canter through the Internet, as I do, you will find many gadgets to help you manage your passwords. It can be something simple like the $7 Login Locker, a tiny Rolodex for your pocket, or a fancy electronic gadget like Password Safe or OnlyKey and many more. If you feel like you want to invest in something more than a pen and paper then feel free to shop around, but remember whatever you choose, the responsibility of physically protecting it will always be there.

If you know an elderly person who is facing these challenges, please share this information and keep them safe.

References: CaregiverStress, SeniorSafetyAdvice, Quora,

Other Interesting News and Cyber Security bits:

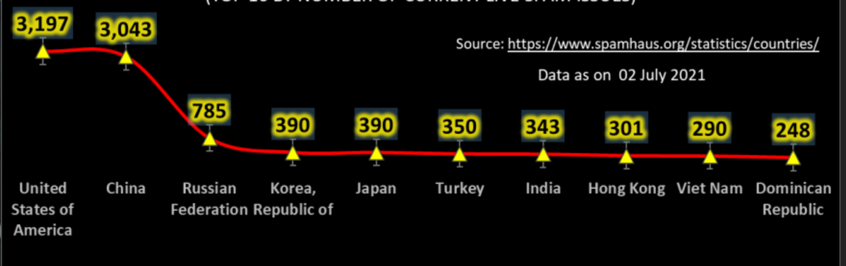
- Should ransomware payment be illegal? It's complicated
- Attacks Erase Western Digital Network-Attached Storage Drives.
- Russian Soyuz-2.1b rocket with 36 British satellites blasts off from Vostochny spaceport

THE WORLD'S WORST SPAM HAVEN COUNTRIES FOR ENABLING SPAMMING

(TOP 10 BY NUMBER OF CURRENT LIVE SPAM ISSUES)

Source: https://www.spamhaus.org/statistics/countries/

Data as on 02 July 2021



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