On September 29, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded). Organizations and users are advised to update and apply all appropriate vendor security patches to vulnerable systems and to continue to update their antivirus signatures daily.
CIS Security Advisories

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
30 September 2022

In The News This Week

Australia asks FBI to help find attacker who stole data from millions of users (Optus Breach)

Attorney general Mark Dreyfus yesterday revealed the FBI was asked to help identify the entities involved in the attack, which saw Optus leak data describing over ten million account holders. Data suspected to have been accessed included drivers licence details, passport numbers, email addresses and phone numbers. Optus, owned by Singaporean mega-telco Singtel, disclosed the breach last Thursday. In the days since, unpicking just what happened has become harder.... An entity claiming to have perpetrated the hack posted a demand for a $1 million ransom to the notorious BreachForums. Australian infosec reporter Jeremy Kirk contacted the poster, who provided some data that Kirk verified as containing records of Optus customers. Kirk later revealed that the entity had released 10,000 records and promised to release more. Kirk also revealed that the data he had seen included references to Medicare, Australia's national public health insurance scheme. Ministers quickly noted that Optus had not previously disclosed the leak of Medicare data...
Read the rest of the story by Simon Sharwood here: The Register

Researchers Identify 3 Hacktivist Groups Supporting Russian Interests

At least three alleged hacktivist groups working in support of Russian interests are likely doing so in collaboration with state-sponsored cyber threat actors, according to Mandiant. The Google-owned threat intelligence and incident response firm said with moderate confidence that "moderators of the purported hacktivist Telegram channels **'XakNet Team**,' **'Infoccentr**,' and **'CyberArmyofRussia_Reborn**' are coordinating their operations with Russian Main Intelligence Directorate (GRU)-sponsored cyber threat actors." Mandiant's assessment is based on evidence that the leakage of data stolen from Ukrainian organizations occurred within 24 hours of malicious wiper incidents undertaken by the Russian nation-state group tracked as APT28 (aka Fancy Bear, Sofacy, or Strontium)... Read the full story by Ravie Lakshmanan: The Hacker News

UK ICO reprimands 7 organisations for failing to adhere to UK GDPR Subject Access Request laws

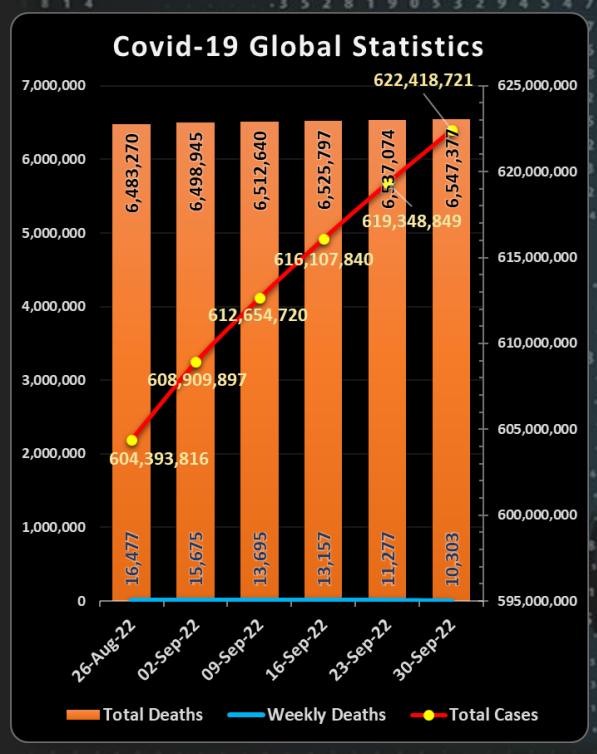
The UK's Information Commissioner's Office (ICO) has announced that it has acted against seven UK organisations for failing to respond to the public when asked for personal information held about them. Organisations must respond to a Subject Access Request (SAR) under Article 15 of the UK GDPR within one to three months, but an ICO investigation found seven organisations across the public and private sectors repeatedly failed to meet this legal deadline. This has resulted in regulatory action including reprimands as well as practice recommendations issued under the Freedom of Information Act 2000 (FOIA). In a posting on its website, the ICO stated that the seven organisations were identified following a series of complaints in relation to multiple failures to respond to requests for copies of personal information collected and processed, either within statutory timeframes or at all, breaching the UK GDPR and Data Protection Act. The seven organisations the ICO has reprimanded are: The Ministry of Defence (MoD), The Home Office, The London Borough of Croydon, Kent Police, The London Borough of Hackney, The London Borough of Lambeth & Virgin Media. Read the story by Michael Hill here: CSO

South Africa- SA ill-equipped for cyberwarfare – with limited money, manpower, and tech expertise

South Africa remains vulnerable to cyberwarfare, despite a plan to protect the country against threats to its national security and commercial capability being put into motion almost eight years ago. Cyberattacks have increased at a rapid rate. The private sector isn't the only target of global cybercriminals. South Africa's state-owned rail, port, and pipeline company, Transnet, became a victim of a ransomware attack in 2021. The country's justice department was also targeted later that same year. These attacks, focused on South Africa's critical infrastructure, are expected to increase in frequency and veracity, according to technology experts. Government approved the National Cybersecurity Policy Framework (NCPF) in 2012, making it official through a gazette three years later... Read the full story by Luke Daniel here: BusinessInsider

Anonymous launches multiple cyber attacks against the Iranian government (Update from last week)

- Hacktivist group, Anonymous, is known to take sides during major world conflicts and it looks like their latest cause is the women of Iran. The death of an innocent woman, Mahsa Amini, has rightly sparked mass nationwide protests in the country. On September 20, the hacking group, Anonymous, announced that it was launching a 'cyber operation' against the Iranian government, under the hashtag #OpIran. The next day, the two main websites of the Iranian government and several state media websites were taken down by hackers claiming to be from Anonymous. One was the 'smart services' website of the government, where a host of online services were offered and another published government news and interviews with officials. 'The largest Iranian media is getting hacked,' said a tweet from the collective's official Twitter account, claiming responsibility for the attack. Several other websites, including the webpage of Iranian state television. Anonymous also claimed to have taken down Iran's Central Bank and Fars News Agency. With protests raging on, the people of Iran have been subjected to ongoing internet blackouts as the government tried to curb further demonstrations...
Read the full story by Anugraha Sundaravelu here: Metro



For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud

Public Wi-Fi Hotspot Security

Now that the Covid-19 restrictions are relaxing in more and more counties, people are starting to travel again and our airports are filling up. With that comes the inconvenience of not having your secure home or work network available, and at some point or another, you'll need to connect to a public Wi-Fi hotspot to access the Internet. Today I want to share an extract of some safe travel tips posted by Eric Griffith for PCMag that might help if you are that traveller.

Avoid the Scammers: Tips for Public Wi-Fi Hotspot Security

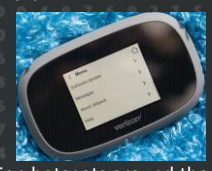
Public Wi-Fi hotspots can be a hacker's paradise. Following these basic security tips can mean the difference between safe surfing and an ID theft or data-loss nightmare. People are addicted to free Wi-Fi. They need it, they crave it, and they don't think twice about connecting to any network that can get them online in most cases. Getting Wi-Fi in a hotel, on an airplane, or even in a restaurant or bar drives decision-making on where to go and stay. Many people even use public Wi-Fi in hotels/rentals to watch adult content—and I'm not talking about HBO Max. Yet most people can't tell a secure Wi-Fi network from an insecure one.
For many, public Wi-Fi hotspots are too convenient to ignore. But they're risky, especially because it's not that hard to make sure you're secure. Some of the tips below involve common sense; the rest you can set up before you leave the house or office. Make sure the next hotspot you connect to—be it in a café or in the sky—isn't a security nightmare waiting to happen.

(1) Pick the Correct Network - Have you ever tried to connect to public Wi-Fi and seen multiple network names that are similar but not the same? EricsCoffeeHaus versus EriksCoffeeHaus, or HiltonGuest versus HiltonGuests, for example. This is a tried-and-true man-in-the-middle attack used by hackers—dubbed Wi-Phishing which tries to trick you into logging into the wrong network to get to your info. Most people don't take the time to check, and jump on the strongest, open signal they see. But you should always check that you pick the legitimate network. Just ask someone who works there for the proper network name if it's not posted.

(2) Pick a Secure Network - When you want to pick a Wi-Fi hotspot to log into, try and find one that's got you locked out. You read that right. Usually, if you see the lock icon, it means you can't get access. Networks with zero security don't have a lock icon next to them, or the word "secured," which shows on a Windows laptop. On an iPhone, if you click an unsecured network—even if it's your own at home—you'll get a warning that reads Security Recommendation.
Of course, this isn't a hard and fast rule. Some hotspots don't show the lock because they have what's called "walled garden" security: You have to log in via a browser to get access to the internet. The login usually is provided by the hotspot—you may get it from the front desk at a hotel, for example, while checking in.
It's best to stick to hotspots where the provider—be it a conference, hotel, or coffee shop—provides you with a clear network to choose from, plus a password to grant access. Then you know at least you're on the network you're meant to be using.

(3) Ask to Connect - You can set most devices to ask for your permission before they connect to a network, rather than just automatically connecting to the strongest open network around, or a network they've connected to before. That's a good idea. Never assume the network you used in one place is as safe as one with the same name in another place. Anyone with the right tools could spoof a Wi-Fi network's broadcast name (called the SSID). If the device asks first, you've got a chance to make a decision about whether it's safe to connect or not. On iOS for example, go to Settings > Wi-Fi > Ask to Join Networks and select Ask. On Android, the exact path will vary, but look for Network & Internet > Wi-Fi preferences in Settings. You want to turn on Open network notification.

(4) Be Your Own Hotspot - Rather than risk everyone in a group using iffy Wi-Fi, one person could designate their own device as the hotspot. Almost all laptops and phones make it easy to become your own hotspot for others. It won't be fast, but it will be more secure. In Windows 10 or 11, turn it on at Settings > Network & Internet > Mobile Hotspot - Copy the name of the network to hand out to people, and give them the network password they need for access (preferably verbally).
On macOS, go to Apple Menu > System Preferences > Sharing and click the Internet Sharing box. Pick a connection type to share, and how you plan to share it (Wi-Fi, duh), then click Wi-Fi options to name your Mac hotspot and give it a password.



(5) Take a Hotspot With You - Public access Wi-Fi is great, but you could just carry your hotspot with you. Cellular modem hotspots have their own battery, use cellular backhaul for an internet connection, and provide multiple people with Wi-Fi access. Sure, it costs more, but it might be worth it if you've got a lot of traveling ahead. Our top pick depends on your carrier (see our roundup of the Best Mobile Hotspots). Overall, this is a lot more secure than using publicly provided Wi-Fi. But it will cost you more, either in money or data (or both). (*Check in your own country what is available, e.g. Telkom or MTN in South Africa*)

(6) Subscribe to Hotspots - Services like Boingo which partners with others to provide access to over 1 million hotspots around the globe—or Gogo which provides hotspots specifically for planes in flight, are two of the big names in subscription Wi-Fi services. Pay them a monthly fee—which can get pricey—and you know when you find their certified hotspots, they're a lot less likely to be run by the bad guys. (Not impossible, but pretty unlikely.)

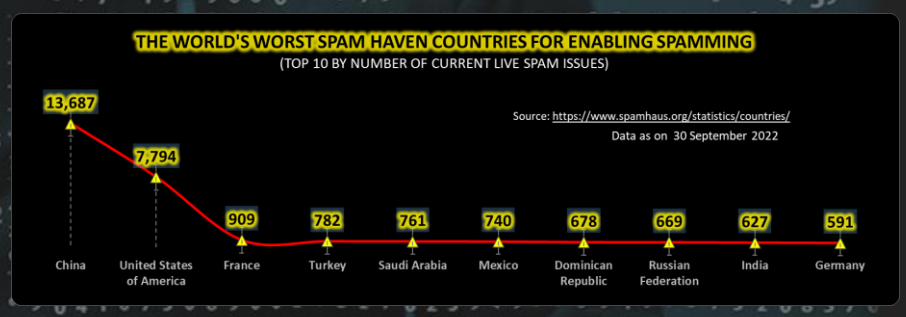
(7) Use Hotspot 2.0 - Never heard of 802.11u? How about Wi-Fi Certified Passpoint? They're all the same thing: A method to help people not only securely get on a hotspot, but roam from supported hotspot to hotspot, cell-tower style. That means you enter credentials to sign in once, which get reused at hotspots all over the place, logging you in instantly and securely. The major operating systems support Hotspot 2.0. For example, in Windows, go to Settings > Network & Internet > Wi-Fi and flip the switch under Hotspot 2.0 networks to turn it on. You can find it in locations with consistent ISP providers like Optimum or Spectrum, or from paid hotspot providers like Boingo. If it's an option for you, use it.

That is all that I have space for in this post but please visit PCMag for 6 more tips on how to use public hotspots securely.

flightradar24 LIVE AIR TRAFFIC Track any Aeroplane in flight globally
Marine Traffic Track any Sailing Vessel globally
SatelliteXplorer Track satellites in orbit

Other Interesting News and Cyber Security bits:

- NASA's DART Mission Hits Asteroid in First-Ever Planetary Defense Test
- Asteroid that crashed into Earth two billion years ago and formed the planet's largest crater in South Africa was up to 15 MILES across - even wider than the one that killed off the dinosaurs
- SANS Daily Network Security Podcast (Storm cast)



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