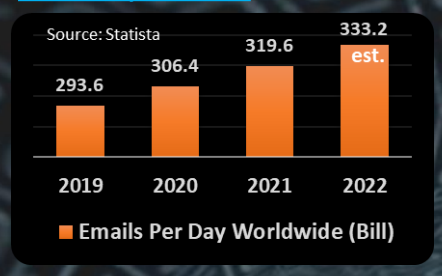
On July 27, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Apple and Mozilla products.
CIS Security Advisories



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

29 July 2022

In The News This Week

Teenager jailed after hacking into Snapchat accounts and demanding money from victims' friends

A teenager has been jailed after hacking into Snapchat accounts to pose as his victims in an effort to make money while threatening to post intimate photos. Jasin Bushi, 18, has been sentenced to two years in prison after admitting to unauthorised access to a computer to facilitate the commission of an offence, fraud by false representation, possession of articles used in fraud and three counts of blackmail. He also pleaded not guilty to three counts of disclosing private sexual photographs or films, with intent to cause distress. Between December 2020 and February 2021, Bushi logged into the Snapchat accounts of seven women, before changing the sign-in details to prevent them regaining access. He then proceeded to pose as his victims and message their friends to ask if he could borrow some money to pay his rent, adding he will be kicked out if he doesn't pay. However, he was sometimes challenged when the victims' friends when they realised something was wrong. Bushi would then double down and admit he wasn't the victim in question, and instead demand money or threaten to send explicit photos of them...
Read the post here: SkyNews

Ukraine's tech excellence is playing a vital role in the war against Russia

Russia's invasion of Ukraine is now in its sixth month with no end in sight to what is already Europe's largest conflict since WWII. In the months following the outbreak of hostilities on February 24, the courage of the Ukrainian nation has earned admiration around the world. Many international observers are encountering Ukraine for the first time and are learning that in addition to their remarkable resilience, Ukrainians are also extremely innovative with high levels of digital literacy. This tech sector strength is driving the Ukrainian response to Russia's imperial aggression. It is enabling the country to defy and in many instances defeat one of the world's leading military superpowers. A start-up culture that owes much to Ukraine's vibrant IT industry is providing rapid solutions to frontline challenges in ways that the more traditional top-down Russian military simply cannot match.... Read the full story by Valeriya Ionan here: Atlantic Council

Social Media data leaks account for 41% of all records breached

Social media is quickly turning into a primary security weak point. A single data breach within one of the major social media networks can result in millions of records being stolen. Within the past few years, we have seen multiple large-scale data breaches involving companies like Facebook and Twitter. Yet, we rarely see the bigger picture. Luckily, data presented by Atlas VPN gives insight into the scope of the issue. It turns out that 41% of all compromised records in 2021 originated from social media data leaks, which is a significant upsurge compared to 25% in 2020. The data presented is based on the 2022 ForgeRock Consumer Identity Breach Report, which gathered data from various sources, such as 2021 Identity Theft Resource Center, IBM Ponemon, TechCrunch, Forrester Research, as well as UpGuard, and IdentityForce.
Read the rest of the article by Edward G. here - AtlasVPN

Ransomware: 1.5 million people have got their files back without paying the gangs. Here's how

No More Ransom project now offers free tools for decrypting 165 families of ransomware as the fight against extortion groups continues. - The battle against ransomware is challenging because not only are ransomware attacks extremely disruptive, but in many cases, victims opt to pay the ransom demand for a decryption key – fuelling additional ransomware attacks because criminals know they can make easy money. However, one scheme continues to take the fight to ransomware gangs and has now helped over 1.5 million victims successfully decrypt their machines without giving into ransom demands, preventing an estimated $1.5 billion from ending up in the hands of cyber criminals. The figures come from Europol on the sixth anniversary of No More Ransom, the European Union law enforcement agency's anti-ransomware initiative.
Read the full story by Danny Palmer here: ZDNet

An Entire Canadian Town Is Being Extorted By Ransomware Cyber Criminals

Ransomware attacks have been on the rise. This time around, the small Ontario, Canada town of St. Marys has been targeted. The ransomware organization behind the attack seems to be LockBit. So far though, no ransom has been paid. The town itself claims that most city functions are still operational and staff are still working and getting paid. Upon visiting the official web site of the town visitors are greeted with a large red box containing the following quote. "The Town of St. Marys is currently investigating a cyber security incident that locked our internal server and encrypted our data. We are working closely with cyber security experts to investigate the source of the incident, restore our back up data, and assess impacts on our information, if any."... Read the rest of the story by Lane Babuder here: HotHardware

EU admits its employees' phones were hacked using Israeli spyware

The European Union found evidence that smartphones used by its staff were compromised by an Israeli company's spy software, says a report citing a letter by the bloc's top justice official. - In a July 25 letter to EU lawmaker Sophie in 't Veld, EU Justice Commissioner Didier Reynders said iPhone maker Apple told him in 2021 that his iPhone had probably been hacked using Pegasus, spyware developed and sold to governments worldwide by Israeli surveillance firm NSO Group, according to a report by Reuters. The letter states that Apple's warning prompted an inspection of the official's personal and professional devices, as well as other phones used by European Commission employees. Although the investigation did not find conclusive evidence that Reynders or EU staff's phones had been hacked, researchers did find "indicators of compromise," a term used by security researchers to describe evidence that hacking had occurred. The letter does not divulge further details and Reynders said it was "impossible to attribute these indicators to a specific perpetrator with full certainty." An NSO spokesman, according to the report, said the company would cooperate with the EU investigation.
Read the full post here: PRESSTV

Smartphone security, it starts with user behaviour

Most of us had either their own phone hacked/compromised or know someone close who had their phone hacked or who fell for a scam. I had a number of post already in this bulletin talking about phone security, and often gave technical guidance on what to do to harden your phone. The truth however, is that most users don't always take the guidance offered to heart and end up being hacked or scammed into something they didn't see coming. Although technical hardening is very important, the main problem, as we are witnessing throughout the world, is human behaviour. In an economically challenged world, it is so easy for criminals to prey on those who are in dire straights, and would grab any opportunity that might offer a solution to their financial needs. We also found that criminals prey on people's emotional needs. As the world rapidly transitioned into a "physically distanced" social media environment during the Covid pandemic, people got lonely and depressed, and they would jump at the slightest chance offered to make it a bit easier. Although the pandemic has been downgraded in most countries, I believe the physical distance transition that happened during the pandemic will stay with us for some time, and the number of depressed people will grow, making the harvest field for criminals even more lucrative. For the criminal, it is not difficult to predict people's behaviour in these circumstances, and they will keep bombarding the phone networks with cleverly crafted campaigns to exploit it. For criminals, it is all about numbers. In an Email campaign for instance, they will send out hundreds of thousands of messages, and if they have a 2% hit rate, it is already worth their while. If you look at the stats posted in the bulletin above, it is estimated that by the end of this year, there will be around **333 billion emails** sent and received every single day. You can do the math, and unfortunately, so can the criminals.

In an effort to come up with some practical advice, I came across this recent ZDNet article by Jack Wallen that brings home what I wanted to put across today. Please see the extract posted below.

Don't want your phone hacked? By Jack Wallen

Every so often I have to dive back into the waters of mobile security and offer up a hard truth for users to swallow. Most often those truths are pretty easy to accept, such as never installing a piece of software unless it's found in the app store for your ecosystem (Google Play Store and the iOS App Store), using a password manager, or always making sure to keep both apps and the operating system updated.

Anyone can follow those best practices. They're simple, harmless, and require very little effort on the part of the user.
But then there are other best practices that aren't quite as easy to follow. Unfortunately, IT admins have had to constantly remind end users to not do certain things for years. And yet, they still happen. No matter how adamant the IT admin is or the consequences of an action might be, end users continue to ignore those warnings, only to wind up having to turn to IT to solve the problems.

When you're dealing with your own personal device, you might not have an IT department to turn to. When that happens, you could wind up having to go to your carrier and pay for the cost of restoring your device to a working condition (which could be costly) or doing a factory restore (which may or may not fix the problem). And then you might have fallen prey to a ransomware attack, at which points all bets are off. Even if you can do a factory restore, your data could be held under the threat of release if you don't pay up. You do not want that.
And this is where probably my most important piece of advice comes into play, with regard to mobile security and it can be summed up with a single, simple phrase. When in doubt, don't.

I have a dear friend who regularly calls me with questions like, "I received this text. I don't know the sender. Should I click on the link?" The answer, unequivocally, is always a resounding "no!" I then remind that person that if they don't know the sender of an email, an SMS message, a Facebook Messenger message, a WhatsApp communication, etc. that they are not to open it, tap it, click it, copy it, respond to it, or otherwise interact with it. And that's the heart of this issue.

So many users (and even publications) want to very quickly lay the blame square on the shoulders of the companies that provide mobile operating systems and/or mobile applications. Not only is that not fair, but it's also not helpful. You see, just like within the realm of desktop and laptop computers, the end user must share the burden of responsibility. Google does not make you tap those links sent to you from unknown sources. Apple has never once twisted your arm to respond to a strange text.

And yet, no matter how many times they are warned, end users continue to tap those strange links and respond to those messages sent by unknown users. The end results could be catastrophic to your data, your privacy, and your identity.

According to Avast, global ransomware attacks are up 32% on businesses and 38% on individuals. Those attacks come in the form of fake package delivery information, tech support scams, sexploitation scams, and phishing scams (when an attacker attempts to trick you into divulging personal information to gain leverage over a victim).

You've seen these emails and SMS messages come into your phones. I get them all the time. While I was writing this article, I received no less than five such scams and my wife forwarded me an email phishing attack that posed as an order for Geek Squad Gold Plus Tech Support at $499.19. Within that email were phone numbers to tap which I guarantee would lead to no end of trouble. I immediately responded to her to say it was a scam and delete it. This type of attack is so common that I've reached the point where I automatically block (or mark as Junk) any email that includes certain phrases or companies that are frequently used in Phishing scams.

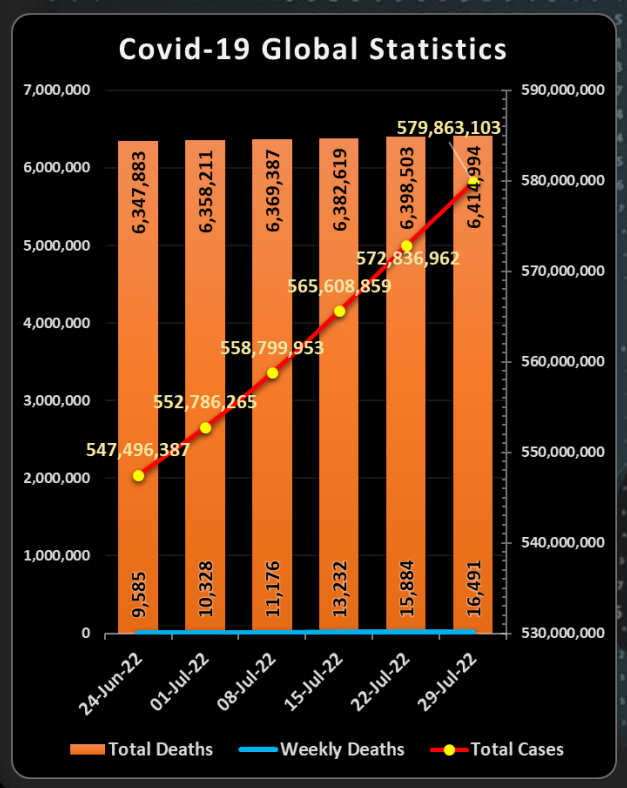
I also receive about 10 SMS messages a day on my phone that goes something like this:
Hey, I tried to call you but you're not answering. What's up?

The sender of that message is not on my contact list which means I don't know them. Over the past few years, I've developed a simple rule: If I don't know you I won't answer the phone or reply to your messages. Now, I don't hesitate to block and report those messages as spam. The sender may be legitimate, but I'm not taking my chances.

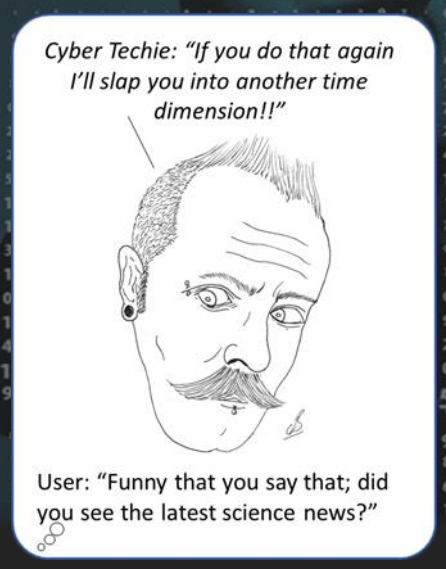
And that's the attitude every mobile user should adopt. Err very well on the side of caution and you'll avoid a lot of common attacks on your privacy and data.

And that, my dear friends, is the hard and simple truth about phone security that you (and everyone you know) need to accept.

Resources: ZDNet

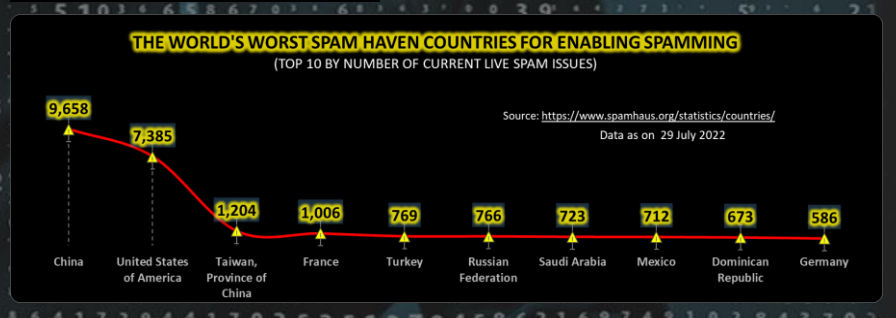


For Reporting Cyber Crime in the USA go to (IC3) , in SA go to Cybercrime, in the UK go to ActionFraud



Other Interesting News and Cyber Security bits:

- Broadcom Survey Shows Security Clash With User Experience
- Hackers scan for vulnerabilities within 15 minutes of disclosure
- What is World of Haiku - the first video game that teaches real-world cybersecurity skills
- New Phase of Matter Opens Portal to Extra Time Dimension
- SANS Daily Network Security Podcast (Storm cast)



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