Cyber Guardian

A PUBLICATION FOR YOUR ONLINE SAFETY

VOLUME 128 | ISSUE 128 15 March 2022

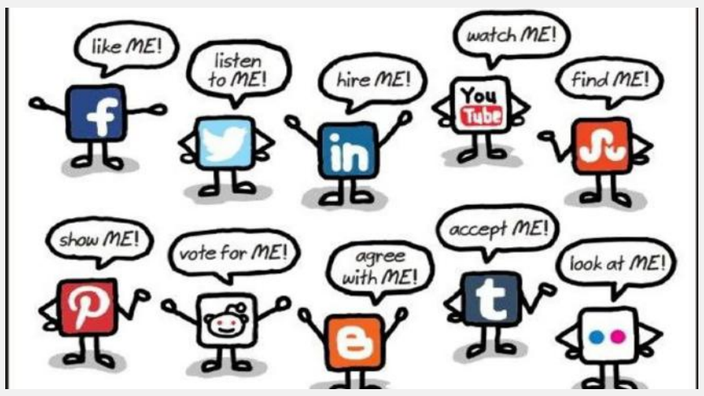
Article of the Month

Tips to maintain your mental health on social media without being a victim of cyberspace

Introduction

Nowadays, people spend an increasing amount of time on social media. Therefore, it's more important than ever to take care of their mental health. Last few months, we heard some shocking facts around the world that most individuals, especially teenagers have faced anxiety problems while using social media. When it comes to the recent mental health day we passed a few months ago, an international holiday that highlighted the significance of mental health to convey about positive adaption. However, let's just not stick to a day to discuss mental issues on social media rather we should more focus on our mental health as a habit to avoid being a victim of major social media problems such as cyberbullying, suicide attempts, etc.

It is also coming to attention that most of the social issues have been raised over psychological addiction and other problems which reminds us that our mental health deserves extra attention in our era of social media. Let's examine a recent survey conducted before the COVID-19 pandemic by the Royal Society for Public Health (RSPH) titled "Social media and young people's mental health and wellbeing"



RSPH has described social media as more addictive than cigarettes and alcohol. Rates of anxiety and depression in young people have risen 70% in the past 25 years, as has poor sleep. Cyberbullying is also a growing problem, with 7 in 10 young people saying they have experienced it. So, with 91% of 16 to 24-year-olds using the internet for social networking, it's essential to practise self-care, both on and offline. Let's examine another recent survey conducted across undergraduates from universities in Shanghai who participated in an online survey which was titled "Problematic Social Media Usage and Anxiety Among University Students During the COVID-19 Pandemic"

Those results also showed that problematic social media usage among university students predicted their levels of anxiety. Considering the above survey facts, you may understand that improper usage of social media has been affected unsatisfactorily on mental health. Though many of us enjoy staying connected on social media, excessive social media usage can fuel feelings of anxiety, depression, isolation, FOMO (Fear of missing out), Self-absorption, Cyberbullying, etc.

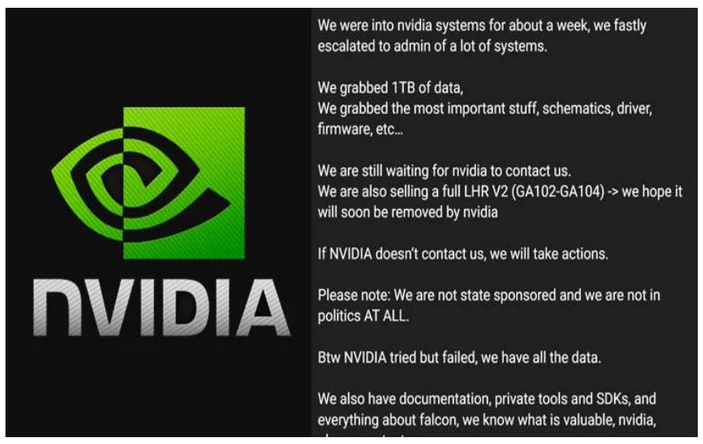
Social media anxiety

A recent Facebook study published in Wall Street Journal says that Instagram can harm the mentality of teens, especially girls. The survey states that 32% of teenage girls say Instagram makes them feel worse when they are in a bad mood. Among the frequently mentioned reasons for stresses were unrealistic beauty and feelings of inadequacy about their current living status compared to those shown on the screen. Instagram has tried to deal with some of these problems by introducing various functions to overcome these issues. Hiding the likes counter or prohibiting filters that show unrealistic beauty standards were among them.

In any case, if someone feels bad, there are also simple steps any user can take:

Around the World

Hackers Who Broke Into NVIDIA's Network Leak DLSS Source Code Online



"...American chipmaking company NVIDIA on Tuesday confirmed that its network was breached as a result of a cyber attack, enabling the perpetrators to gain access to sensitive data, including source code purportedly associated with its Deep Learning Super Sampling (DLSS) technology. "We have no evidence of ransomware being deployed on the NVIDIA environment or that this is related to the Russia-Ukraine conflict," the company said in a security notice. "However, we are aware that the threat actor took employee passwords and some NVIDIA proprietary information from our systems and has begun leaking it online." The incident is said to have come to light on February 23, with the company noting that it's taken steps to analyze the leaked information and that it's enforcing all of its employees to change their passwords with immediate effect.The confirmation comes days after The Telegraph last week reported that the company is investigating a potential cyber attack that took "parts of its business offline for two days." Bloomberg, in a follow-on report, said the breach was a minor ransomware attack, citing a "person familiar with the incident." ....."

Researchers Demonstrate New Side-Channel Attack on Homomorphic Encryption

"...A group of academics from the North Carolina State University and Dokuz Eylul University have demonstrated what they say is the "first side-channel attack" on homomorphic encryption that could be exploited to leak data as the encryption process is underway. "Basically, by monitoring power consumption in a device that is encoding data for homomorphic encryption, we are able to read the data as it is being encrypted," Aydin Aysu, one of the authors of the study, said. "This demonstrates that even next generation encryption technologies need protection against side-channel attacks." Homomorphic Encryption is a form of encryption that allows certain types of computation to be performed directly on encrypted data without having to decrypt it in the first place.It's also meant to be privacy-preserving in that it allows sharing of sensitive data with other third-party services, such as data analytics firms, for further processing while the underlying information remains encrypted, and by extension, inaccessible to the service provider. Put differently, the goal of homomorphic encryption is to facilitate the development of end-to-end encrypted data storage and computation services where the data owner never needs to share their secret keys with third-party services....."

The most impersonated brands in phishing attacks

• Always try to reduce the time you spend online on social media or similar platforms.

• Unsubscribe from accounts that make you feel unconfident, upset, inadequate or sad.

• Take slight breaks to escape from social networks and try to relax and focus on yourself.

Cyberbullying

Cyberbullying is another notable issue that could affect teens' mental health. If someone is being bullied, well, that's something you should not be tolerated or ignored. If the victim is a teen who is being bullied online, the first step you can take is to get help from parents or someone you could trust adult, like a school teacher or counsellor. If the victim is an adult or even a teen, and you both are uncomfortable finding a trustable person nearby, then seek help from a professional in the field. The victim always can contact a helpline and talk to a professional consultant.

At present, most social networks actively use AI to combat abusive comments in pictures and videos. Each social platform also provides mechanisms to customize who can comment on your posts or view your posts. Those platforms also provide ways to block users and report cases of bullying or intimidation. Anyway, it's better if you can collect evidence such as screenshots, URLs to confirm what is happening.

The positive aspects of social media

Although virtual social media interactions don't have the same psychological benefits as face-to-face contact, there are still many positive ways they can help you stay connected and maintain your well-being.

Social media allows you to:

• Communicate and stay connected with family and friends around the world.

• Find new friends and communities that share similar interests and ambitions.

• Find a platform for your creativity and self-expression.

• Discover sources of valuable information and learning.

• Join or promote worthwhile causes by raising awareness on important issues.

• Seek emotional support for yourself during your tough times.

• Offer emotional support for others during their hard times.

• Find a vital social connection if you live in a remote area, have limited independence, experience social anxiety, or are part of a marginalized group.

If social media is affecting your mental health, it's important to talk to someone. This could be a relative, friend, or someone you are close to and trust. Pay attention to how social media affects other aspects of your life, such as eating, sleeping, and focusing. If the victim's mental condition continues to deteriorate, contact a specialist immediately.

Main national level institutes which act against cyber frauds. Below is a brief description of each of them.

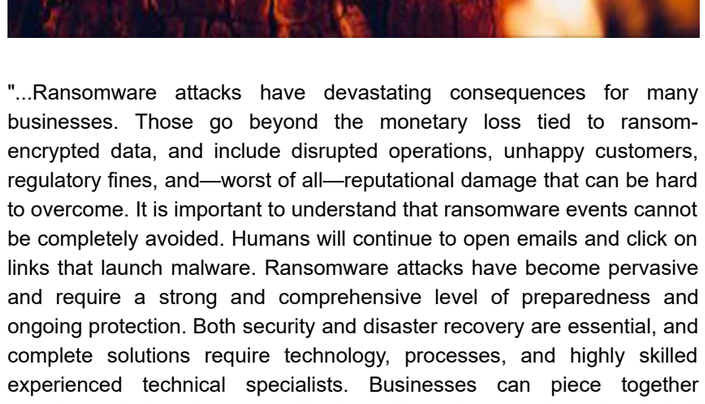
Criminal Investigation Department (CID) – Social Media Unit

"...Vade announced its annual ranking of the top 20 most impersonated brands in phishing. Facebook, which was in the second spot in 2020, rose to the top spot for 2021, representing 14% of phishing pages, followed by Microsoft, with 13%. The report analyzed 184,977 phishing pages linked from unique phishing emails between January 1, 2021 and December 31, 2021. With six brands in the top 20, financial services was the most impersonated industry of 2021, representing 35% of all phishing pages, rising sharply based on its place at 28% in 2020. Chase, PayPal, and Wells Fargo join the list of the most impersonated financial services brands.Microsoft is the second most impersonated brand in phishing attacks and the #1 most impersonated cloud brand, coming in just slightly behind Facebook. The report found that Microsoft phishing attacks sharply increased in sophistication in 2021, with a June attack leveraging automation to populate corporate logos and branding onto Microsoft 365 phishing pages. Joining Microsoft on the list of impersonated cloud brands are Netflix (#12) and Adobe (#15)....."

What is Ransomware Protection as a Service?

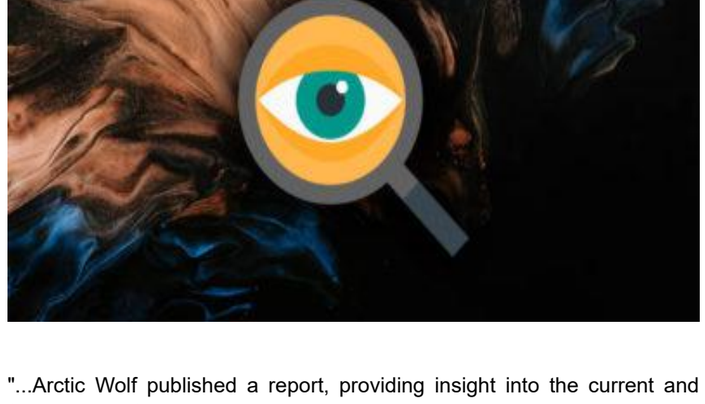
"...Ransomware attacks have devastating consequences for many businesses. Those go beyond the monetary loss tied to ransom-encrypted data, and include disrupted operations, unhappy customers, regulatory fines, and—worst of all—reputational damage that can be hard to overcome. It is important to understand that ransomware events cannot be completely avoided. Humans will continue to open emails and click on links that launch malware. Ransomware attacks have become pervasive and require a strong and comprehensive level of preparedness and ongoing protection. Both security and disaster recovery are essential, and complete solutions require technology, processes, and highly skilled experienced technical specialists. Businesses can piece together complete solutions but generally do not have the experienced technical specialists to pull them off, as they are in very short supply and very expensive to hire. Ransomware Protection as a Service (RPaaS) has emerged to provide full coverage both before and after a ransomware event. Here, the preventative and restorative sides of the equation are paired under a single service, along with detection solutions to bridge the two areas....."

Perennial security challenges hampering organizations in achieving their security objectives



"...Arctic Wolf published a report, providing insight into the current and future state of cybersecurity teams as they attempt to move their security programs forward while dealing with an ever-evolving threat environment. Ongoing security concerns such as ransomware, phishing and vulnerabilities don't just monopolize headlines, they're taking up security professionals' headspace, too. Incessant threats from attackers with far more resources feels like a lost cause. Shifting security strategies to operationalize resources, optimize talent and weaponize defenses is the way forward to deterring attackers and minimizing risk.70% of new customers surveyed are found to have existing latent threats when they are onboarded 81% of respondents rated vulnerabilities and unknown misconfigurations as the biggest security concerns within their environments 50% of organizations say their security budget in 2022 is lacking in a way that will not let them achieve their security objectives, and 30% of organizations with cyber insurance who were surveyed say their policy costs went up or were cancelled outright in 2021, while 35% of organizations currently operate without any form of cyber insurance....."

Every business is a cybersecurity business



"...Hybrid working, with some staff dialing in remotely and others based in the office, forms the basis of how many organizations work, yet many businesses are still not fully equipped for the inevitable security risks that decentralization creates. Surprisingly, despite 39% of UK businesses reporting cybersecurity breaches within the past 12 months, only 23% have a security policy in place that explicitly covers home working.Despite the shift to online work, many businesses remain behind the curve with their longer-term cybersecurity strategies. The challenge is to implement measures that are easy for employees to understand and use, but difficult for malicious actors to exploit. While IT leaders must be at the forefront of building a cybersecurity strategy, securing remote work is no longer just a task for IT. It's up to the entire C-suite to foster a company-wide culture of security and trust, which requires a level of understanding and responsibility from all employees. This is not just a technological challenge, but an educational one....."

Cyber-criminal complaints that are clearly mentioned with relevant evidence (correct links, screenshots, etc.) can be handed over to the CID, or sent to “The Director, Criminal Investigation Department, Colombo 01” by registered post. Additionally, you have the option of emailing the same via: dir.cid@police.lk

Phone: 011 233 7432
Website: https://www.police.lk/index.php/item/719-criminal-investigation-department

Sri Lanka Computer Emergency Readiness Team | Coordination Centre (Sri Lanka CERT|CC)

Sri Lanka CERT|CC is one of the main institutes which provide cyber security emergency responses. It also supports the Sri Lanka Police to resolve the complaints you made regarding cyber security. To protect Information Technology users in the Public and Private Sector Organizations and the General Public by providing up-to-date information on potential threats and vulnerabilities and by undertaking computer emergency response handling services. Here are the contact details:

Place a complaint here: https://cert.gov.lk
Room 4-112, BMICH, Bauddhaloka Mawatha, Colombo 07, Sri Lanka.
Phone: +94 11 269 1692 / 269 5749 / 267 9888
Fax: +94 11 269 1064

TechCERT

TechCERT is a division of LK Domain Registry and has its origins in a pioneering project of the LK Domain Registry with academic partners to provide computer emergency response services to the public and private sector institutions in Sri Lanka. TechCERT has collaborative partnerships with several national and global information security organisations that provide latest data on computer and network security threats and vulnerabilities.

Address: TechCERT, 1st Floor, Bernards Business Park, 106, Dutugemunu Street, Kohuwala
Hot line: +94114219125, 0114-462562 (hotline)
Fax: +94112650805
Email: info@techcert.lk
Web: www.techcert.lk

Other Institutes you can contact for help….

• Police Emergency
Phone: 119
Email: www.telligp.police.lk
Website: https://www.police.lk/index.php/item/15

• Police Emergency
Phone: 119
Email: www.telligp.police.lk
Website: https://www.police.lk/index.php/item/15

• Police Child & Women Bureau
Phone: 011 244 4444
Email: cwbureau@police.lk
Website: https://www.police.lk/

• Child Helpline – National Child Protection Authority (NCPA
Phone: 1929
Email: ncpa@childprotection.gov.lk
Website: http://www.childprotection.gov.lk/?page_id=6

• Women Helpline – Ministry of Women & Child Affairs
Phone: 1938
Email: secncwsl@gmail.com
Website: http://www.childwomenmin.gov.lk/institutes/national-committee-women/1938-womens-help-line

• Women In Need (WIN)s
Phone: 077 567 6555, 077 734 9100, 011 267 1401-11, 011 461 5549
Email: connect@winsl.net
Website: https://www.winsl.net/

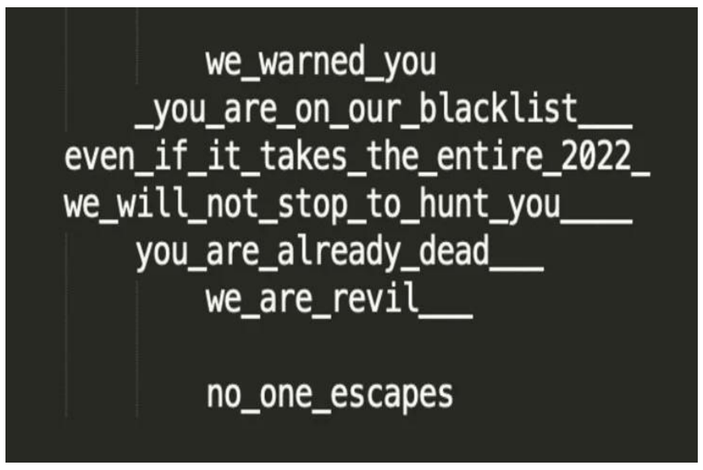
• Special Mental Health Hotline
Phone: 1926
Email: info@nimh.health.gov.lk
Website: http://nimh.health.gov.lk/

• Sumithrayo
Phone: 011 268 2535, 011 268 2570
Email: info@srilankasumithrayo.lk
Website: https://srilankasumithrayo.lk/

• Telecommunications Regulatory Commission (TRC) – Police Unit
Phone: 011 267 1676
Email: investigation@trc.gov.lk
Website: http://www.trc.gov.lk/

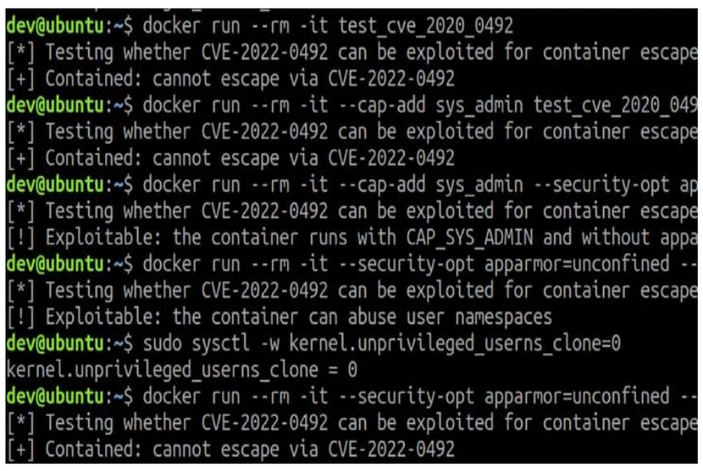
• Government Information Center (GIC)
Phone: 1919 (Dial from abroad: +94 11 2 191919)
Website: http://gic.gov.lk/

Imperva Thwarts 2.5 Million RPS Ransom DDoS Extortion Attacks



"...Cybersecurity company Imperva on Friday said it recently mitigated a ransom distributed denial-of-service (DDoS) attack targeting an unnamed website that peaked at 2.5 million requests per second (RPS). "While ransom DDoS attacks are not new, they appear to be evolving and becoming more interesting with time and with each new phase," Nelli Klepfish, security analyst at Imperva, said. "For example, we've seen instances where the ransom note is included in the attack itself embedded into a URL request." The top sources of the attacks came from Indonesia, followed by the U.S., China, Brazil, India, Colombia, Russia, Thailand, Mexico, and Argentina. Distributed denial-of-service (DDoS) attacks are a subcategory of denial-of-service (DoS) attacks in which an army of connected online devices, known as a botnet, is used to overwhelm a target website with fake traffic in an attempt to render it unavailable to legitimate users.The California-headquartered firm said that the affected entity received multiple ransom notes included as part of the DDoS attacks, demanding the company make a bitcoin payment to stay online and avoid losing "hundreds of millions in market cap."....."

New Linux Kernel cgroups Vulnerability Could Let Attackers Escape Container



"...Details have emerged about a now-patched high-severity vulnerability in the Linux kernel that could potentially be abused to escape a container in order to execute arbitrary commands on the container host. The shortcoming resides in a Linux kernel feature called control groups, also referred to as cgroups version 1 (v1), which allows processes to be organized into hierarchical groups, thereby making it possible to limit and monitor the usage of resources such as CPU, memory, disk I/O, and network. Tracked as CVE-2022-0492 (CVSS score: 7.0), the issue concerns a case of privilege escalation in the cgroups v1 release_agent functionality, a script that's executed following the termination of any process in the cgroup. "The issue stands out as one of the simplest Linux privilege escalations discovered in recent times: The Linux kernel mistakenly exposed a privileged operation to unprivileged users," Unit 42 researcher Yuval Avrahami said in a report published this week.Whether or not the release_agent program is invoked when a particular cgroup becomes empty is determined by the value in the notify_on_release file in the corresponding cgroup directory. If this file contains the value 0, then the release_agent program is not invoked. If it contains the value 1, the release_agent program is invoked. The default value for this file in the root cgroup is 0....."

2 New Mozilla Firefox 0-Day Bugs Under Active Attack — Patch Your Browser ASAP!

"...Mozilla has pushed out-of-band software updates to its Firefox web browser to contain two high-impact security vulnerabilities, both of which it says are being actively exploited in the wild. Tracked as CVE-2022-26485 and CVE-2022-26486, the zero-day flaws have been described as use-after-free issues impacting the Extensible Stylesheet Language Transformations (XSLT) parameter processing and the WebGPU inter-process communication (IPC) Framework.XSLT is an XML-based language used for the conversion of XML documents into web pages or PDF documents, whereas WebGPU is an emerging web standard that's been billed as a successor to the current WebGL JavaScript graphics library.Use-after-free bugs – which could be exploited to corrupt valid data and execute arbitrary code on compromised systems – stem mainly from a "confusion over which part of the program is responsible for freeing the memory."Mozilla acknowledged that "We have had reports of attacks in the wild" weaponizing the two vulnerabilities but did not share any technical specifics related to the intrusions or the identities of the malicious actors exploiting them.Security researchers Wang Gang, Liu Jialei, Du Sihang, Huang Yi, and Yang Kang of Qihoo 360 ATA have been credited with discovering and reporting the shortcomings. While targeted attacks leveraging zero-days in Firefox have been a relatively rare occurrence when compared to Apple Safari and Google Chrome, Mozilla previously addressed three actively exploited flaws in ....."

References

[1] Shttps://www.unicef.org/romania/stories/five-tips-maintain-your-mental-health-while-using-social-media

[2] https://www.helpguide.org/articles/mental-health/social-media-and-mental-health.htm

[3] https://www.frontiersin.org/articles/10.3389/fpsyg.2021.612007/full

[4] https://patient.info/news-and-features/how-to-look-after-your-mental-health-on-social-media

[5] https://www.hithawathi.lk/how-to-get-help/useful-contact-information

[6] https://www.hithawathi.lk/how-to-get-help/what-you-should-do

By:

Shehan Sanjula

Shehan is an Undergraduate of Sri Lanka Institute of Information Technology, who is currently following Bachelor of Sience Honours in Information Technology Specializing in Cyber Security degree program. Currently, he is working as an Intern - Application Security at Sri Lanka CERT|CC.

Critical Bugs in TerraMaster TOS Could Open NAS Devices to Remote Hacking

"...Researchers have disclosed details of critical security vulnerabilities in TerraMaster network-attached storage (TNAS) devices that could be chained to attain unauthenticated remote code execution with the highest privileges. The issues reside in TOS, an abbreviation for TerraMaster Operating System, and "can grant unauthenticated attackers access to the victim's box simply by knowing the IP address, Ethiopian cyber security research firm Octagon Networks' Paulos Yibelo said in a statement shared with The Hacker News. TOS is the operating system designed for TNAS appliances, enabling users to manage storage, install applications, and backup data. Following responsible disclosure, the flaws were patched in TOS version 4.2.30 released last week on March 1, 2022. ....."

Brought to you by:

Sri Lanka Computer Emergency Readiness Team | Coordination Centre

Room 4-112, BMICH, Bauddhaloka Mawatha,

Colombo 07

Tel. +94 - 112 691 692

www.cert.gov.lk