

COVID-19 RELATED CYBER NEWS

Week 9: Saturday 13th June to Friday 19th June
Compiled by Barry Gooch

COUNTRIES WITH OFFICIAL TRACK & TRACE APPS

You will be aware that Google and Apple have developed track and trace apps, and that a number of Countries also have developed and deployed official apps (listed below).

Please bear in mind that many unofficial apps also exist. For example, in the UK King's College London, Guy's and St Thomas' Hospitals, with Zoe Global Limited have developed an app which is being used to study symptoms.

Australia

COVIDSafe is a digital contact tracing app announced by the Australian Government on 14 April 2020 based on the BlueTrace protocol developed by the Singaporean Government.

Azerbaijan

e-Tabib is an official contact tracing and informational mobile app.

Bahrain

BeAware Bahrain is the official mobile app for Android and iOS.

Bangladesh

Corona Tracer BD launched in May 2020 through Play Store.

China

The Chinese government deployed an app in the Shanghai area an app called **Go Together**, and a similar app in the Beijing area called **To Help With Care**. They are in use across more than 200 Chinese cities.

Colombia

CoronApp is the mobile app for Android and iOS –and available for the Huawei AppGallery– developed by the Colombian government. CoronApp incorporates technologies such as those developed by the Governments of Singapore and South Korea, as well as Apple.

Czech Republic

The government launched a Singapore-inspired tracing app called eRouška (**eFacemask**). The app was developed by the local IT community, released as open-source software and will be handed over to the government.

France

StopCovid was released 2 June 2020 to help combat the COVID-19 pandemic. StopCovid is a digital contact tracing app based on a bluetooth tracing protocol developed specially for the app.

Germany

Corona-Warn-App was made available for download on June 16th, 2020. It was developed as open-source software jointly by Deutsche Telekom and SAP with scientific advice from the federal Robert Koch Institute and uses the Exposure Notification APIs from Google and Apple.

Ghana

GH Covid-19 Tracker App, is an Android and IOS app equipped with location tracking technology to provide detailed information about people who have been at the same event, location, country or other defined locations.

Hungary

VirusRadar, an Android app, was launched on May 13 and an iOS version on May 30, 2020. The app uses Bluetooth technology and was developed by Nextsense, based on the company's contact tracing technology.

Iceland

Rakning C-19 route tracking is a GPS logger app for Android and iOS, with a user interface and content from the national COVID-19 web page.

India

The **Aarogya Setu** app is developed by the National Informatics Centre and is available on Google Play Store and Apple's App Store for download.

Israel

On March 22, 2020 the Ministry of Health launched **HaMagen**, an iOS and Android contact tracing app.

Italy

On June 1, 2020 the Italian Government's exposure notification solution, **Immuni** an iOS and Android contact tracing app build on top of the Google/Apple API was launched.

Japan

On June 19, 2020 Japan released COVID-19 Contact-Confirming Application known as **Shingata Koronauirusu Sesshoku Kakunin Apuri, COCOA**. It is available on iOS 13.5 or above and Android 6 or above.

Jordan

The **AMAN App** - was released on May 21, 2020 and is currently available on Google Play Store and App Store.

Latvia

A consortium of IT companies and volunteers launched decentralized proximity tracing **Apturi Covid** application on May 29th, 2020. It is Android and Apple compatible.

Malaysia

The government launched **MyTrace** on May 3, 2020, one of three tracing app that released alongside **Gerak Malaysia** and **MySejahtera**. Gerak Malaysia is a tracing app which allows police and the Ministry of Health to track and analyze users movement and register for permission to allow state border crossing. MySejahtera is an app build by the National Security Council and the Ministry of Health to retrieve updated information and statistics of the pandemic. MyTrace is a tracing app that utilizes Bluetooth to detect how long a user smartphone are in close proximity with other smartphone users with a similar app installed and is currently available on Android.

New Zealand

The Health Ministry launched the **NZ COVID Tracer** on 20 May. The app is available on Apple's App Store and Google Play.

North Macedonia

The government launched the Bluetooth app **StopKorona!** on April 13, 2020.

Norway

The **Smittestopp** app is developed by the Norwegian government and uses Bluetooth and GPS signals. On June 15, 2020, the country halted the app over privacy concerns after the Norwegian Data Protection Authority said low infections could no longer justify the risk of privacy invasion by the end user. The app ceased collecting new data and plans to delete all data collected so far with any additional collections effectively paused indefinitely.

Saudi Arabia

Corona Map Saudi Arabia is the official mobile app for Web, Android and iOS, developed by the National Health Information Center (NHIC)

Singapore

An app called **TraceTogether** uses a digital contact tracing protocol called BlueTrace, developed with an open source reference implementation called OpenTrace.

Spain

An app called **OpenCoronavirus** has been developed by a group of volunteers. It uses an uncentralized contact tracing protocol called MFP-3T, based on DP-3T protocol but improved to avoid a few security issues. The app is being used by a few regions.

Switzerland

An app called **SwissCovid** which uses the DP-3T protocol and is build top of Apple/Google bluetooth API. Application is licenced under Mozilla Public License 2.0.

COVID-19 RELATED ARTICLES

MAIN SOURCES	
Bleeping Computer	https://www.bleepingcomputer.com
Bloomberg	https://www.bloomberg.com/europe
BBC i-player technology news	https://www.bbc.co.uk/news/technology
Business Insider	https://www.businessinsider.com/international?r=US&IR=T
CNET	https://www.cnet.com/news/
Cyware	https://cyware.com/cyber-security-news-articles
Dark Reading	https://www.darkreading.com
Fireeye	https://www.fireeye.com
Fraud Watch International	https://fraudwatchinternational.com
The Guardian	https://www.theguardian.com/uk
Hackmageddon	https://www.hackmageddon.com
Help Net Security	https://www.helpnetsecurity.com
Info Security Magazine	https://www.infosecurity-magazine.com
Malwarebytes	https://blog.malwarebytes.com/category/malwarebytes-news/
Naked Security (Sophos)	https://nakedsecurity.sophos.com
Reuters technology news	https://uk.reuters.com/news/technology
Risk IQ	https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/?utm_source=homepage&utm_medium=carousel-covid19-cybercrime-blog
Security Boulevard	https://securityboulevard.com
SC Magazine UK	https://www.scmagazineuk.com
SC Magazine US	https://www.scmagazine.com
Sky News	https://news.sky.com/uk
Threatpost	https://threatpost.com
Wall Street Journal	https://www.wsj.com/news/technology
We Live Security	https://www.welivesecurity.com
ZDnet	https://www.zdnet.com/2/

SATURDAY 13th June 2020

- **COVID-19 accelerates need to deploy physical and digital security measures**
<https://cyberriskleaders.com/covid-19-accelerates-need-to-deploy-physical-and-digital-security-measures/>
- **The cybersecurity and COVID-19 relationship**
<https://www.curatrix.co.uk/cybersecurity-and-covid-19/>
- **Canberra public servants charged with conspiring to defraud Australian Government**
<https://www.abc.net.au/news/2020-06-11/public-servants-charged-with-conspiring-to-defraud-government/12344164>
- **14,429 crores of bank fraud cases registered by CBI in first half of 2020**
<https://www.timesnownews.com/india/article/14429-crores-of-bank-fraud-cases-registered-by-cbi-in-first-half-of/605963>
- **Axis Bank reports e-fraud on coops platform**
http://timesofindia.indiatimes.com/articleshow/76348373.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **Honda resumes production in India post suspected cyber attack**
<https://www.carwale.com/news/honda-resumes-production-in-india-post-suspected-cyber-attack/>
- **Inadequate Investment in Cybersecurity is Behind Increase in Cyber Attacks**
<https://www.itnewsafrika.com/2020/06/inadequate-investment-in-cybersecurity-is-behind-increase-in-cyber-attacks/>
- **Cybercriminals change tack in SA, use more ransomware during lockdown**
<https://www.news24.com/fin24/companies/ict/cybercriminals-change-tack-in-sa-use-more-ransomware-during-lockdown-20200613>
- **Email-borne cyber-attacks are inevitable, says UAE firms**
<https://www.tahawultech.com/industry/technology/email-borne-cyber-attacks-are-inevitable-says-uae-firms/>
- **Check your Canada Revenue Agency account for changes, Ottawa police warn, amid CERB fraud claims**
<https://ottawa.ctvnews.ca/check-your-canada-revenue-agency-account-for-changes-ottawa-police-warn-amid-cerb-fraud-claims-1.4983036>
- **Black Kingdom ransomware hacks networks with Pulse VPN flaws**
<https://www.bleepingcomputer.com/news/security/black-kingdom-ransomware-hacks-networks-with-pulse-vpn-flaws/>
- **Hacker Bypasses GE's Ridiculous Refrigerator DRM**
https://www.vice.com/en_us/article/jgxpjy/hacker-bypasses-ges-ridiculous-refrigerator-drm?&web_view=true
- **SparkCognition and Siemens Join Forces for Industrial Security Solution**
https://www.securityweek.com/sparkcognition-and-siemens-join-forces-industrial-security-solution?&web_view=true
- **Beware of fake apps with malware mimicking TraceTogether**
https://www.straitstimes.com/singapore/beware-of-fake-apps-with-malware-mimicking-tracetoegether?&web_view=true
- **Researcher Demonstrates Android App Hacking via Intents**
https://www.securityweek.com/researcher-demonstrates-android-app-hacking-intents?&web_view=true&web_view=true

- **Russian hacker releases at least 14,000 Mexican taxpayer IDs**
https://www.scmagazine.com/home/security-news/apts-cyberespionage/russian-hacker-releases-at-least-14000-mexican-taxpayer-ids/?&web_view=true
- **Infection At The Click Of A Mouse: There's A New Pandemic And This Time We Are All At Risk**
https://www.forbes.com/sites/carrierubinstein/2020/06/12/infection-at-the-click-of-a-mouse-theres-a-new-pandemic-and-this-time-we-are-all-at-risk/#e088eda73ccd?&web_view=true
- **Critical Vulnerabilities Expose Siemens LOGO! Controllers to Attacks**
https://www.securityweek.com/critical-vulnerabilities-expose-siemens-logo-controllers-attacks?&web_view=true
- **Honda Hackers May Have Used Tools Favored by Countries**
https://www.newsvevo.com/2020/06/13/honda-hackers-may-have-used-tools-favored-by-countries/?&web_view=true
- **COVID-19 impact on migrant smuggling and human trafficking**
<https://www.interpol.int/en/News-and-Events/News/2020/COVID-19-impact-on-migrant-smuggling-and-human-trafficking>

SUNDAY 14th June 2020

- **COVID-19 Cyberthreats Spike in India, Brazil, and the U.K.: Google**
<https://www.cisomag.com/covid-19-related-threats-spike-in-the-u-k-india-and-brazil-google/>
- **The hacker, the faker and the virus**
<https://www.theweek.in/theweek/current/2020/06/04/the-hacker-the-faker-and-the-virus.html>
- **Five Wanted For Indian Crypto Scam Operating Since 2017**
<https://cointelegraph.com/news/five-wanted-for-indian-crypto-scam-operating-since-2017>
- **Sapiens pays \$250,000 in Bitcoin to hackers who took over its computers**
<https://www.calcalistech.com/ctech/articles/0,7340,L-3833070,00.html>
- **Extortionists threaten to destroy sites in fake ransom attacks**
<https://www.bleepingcomputer.com/news/security/extortionists-threaten-to-destroy-sites-in-fake-ransom-attacks/>
- **Attackers impersonate secure messaging site to steal bitcoins**
<https://www.bleepingcomputer.com/news/security/attackers-impersonate-secure-messaging-site-to-steal-bitcoins/>
- **Adding noise for completely secure communication**
https://www.sciencedaily.com/releases/2020/06/200611133116.htm?&web_view=true
- **SGAxe Attacks Chopping off Data From Intel SGX Enclaves**
<https://cyware.com/news/sgaxe-attacks-chopping-off-data-from-intel-sgx-enclaves-26a216df>
- **Thanos Ransomware: Ransomware Protections Bite the Dust**
<https://cyware.com/news/thanos-ransomware-ransomware-protections-bite-the-dust-7a5f3f5d>
- **How Cyber Adversaries Exploit Employee Systems For Their Benefit**
<https://cyware.com/news/how-cyber-adversaries-exploit-employee-systems-for-their-benefit-142880e5>
- **Kingminer Botnet: The Persistent Nuisance**
<https://cyware.com/news/kingminer-botnet-the-persistent-nuisance-38310ee6>
- **Air-Gapped Systems are Becoming a Treasure Trove for Attackers**
<https://cyware.com/news/air-gapped-systems-are-becoming-a-treasure-trove-for-attackers-f109e579>

MONDAY 15th June 2020

- **D'oh! Beer Company Suffers Cyber Attack**
<https://www.natlawreview.com/article/d-oh-beer-company-suffers-cyber-attack>
- **The Evolving Cyber-Security Threat of COVID-19**
<https://www.extremenetworks.com/extreme-networks-blog/the-evolving-cyber-security-threat-of-covid-19/>
- **£250m cyber security framework launched**
<http://www.thehtn.co.uk/2020/06/15/250m-cyber-security-framework-launched/>
- **UNDER ATTACK: 'Largest cyber attack in history' hits all US mobile phone operators sparking outages**
<https://www.thesun.co.uk/news/11871782/ddos-attack-t-mobile-outage-facebook-instagram-us/>
- **ActionSpy used against Uyghurs. Anonymous claims action against Atlanta police. Cybersquatting and phishing. Bogus ransomware.**
<https://thecyberwire.com/newsletters/daily-briefing/9/115>
- **Coronavirus: Enterprise VPN adoption in India set to rise**
<https://www.computerweekly.com/news/252484644/Coronavirus-Enterprise-VPN-adoption-in-India-set-to-rise>
- **How I almost lost thousands after falling for email hacking scam**
<https://www.stuff.co.nz/business/121768194/how-i-almost-lost-thousands-after-falling-for-email-hacking-scam>
- **Hackers targeting working from home security flaws - CERT**
<https://www.rnz.co.nz/news/national/419073/hackers-targeting-working-from-home-security-flaws-cert>
- **Covid-19 disruption side effect: Rise in cybersecurity jobs in India**
https://www.business-standard.com/article/companies/covid-19-lockdown-side-effect-rise-in-cybersecurity-jobs-in-india-120061501450_1.html
- **APAC region still insufficiently prepared for opportunistic cyber-attacks**
<https://www.cybersecasia.net/news/apac-region-still-insufficiently-prepared-opportunistic-cyberattacks>

- **Mobile banking malware that hides in MS Word, Adobe flash apps may affect Android smartphones**
https://economictimes.indiatimes.com/magazines/panache/mobile-banking-malware-that-hides-in-ms-word-adobe-flash-apps-may-affect-android-smartphones/articleshow/75749745.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **Defending the breach: The rising costs of cyber-attacks for companies**
<https://www.lexology.com/library/detail.aspx?g=13005a8f-f975-4f59-bc87-d57229f707d7>
- **South African bank to replace 12m cards after employees stole master key**
<https://www.zdnet.com/article/south-african-bank-to-replace-12m-cards-after-employees-stole-master-key/>
- **47% of South African organisations expect to suffer from an email-borne attack – Report**
<https://businesstech.co.za/news/industry-news/407537/47-of-south-african-organisations-expect-to-suffer-from-an-email-borne-attack-report/>
- **Cyberreason Honeypot Traps Hackers Targeting ICS**
<https://www.cxoinsightme.com/news/cyberreason-honeypot-traps-hackers-targeting-ics/>
- **Nuclear Missile Contractor Hacked**
<https://www.cybersecurityintelligence.com/blog/nuclear-missile-contractor-hacked-5020.html>
- **CYBER-ATTACKS NOT A QUESTION OF ‘IF’, BUT ‘WHEN’**
<https://www.businessinnovationmag.co.uk/cyber-attacks-not-a-question-of-if-but-when/>
- **New Orleans Hotel Owner Charged With Conspiracy to Defraud First NBC Bank**
<https://www.justice.gov/usao-edla/pr/new-orleans-hotel-owner-charged-conspiracy-defraud-first-nbc-bank>
- **Government gives companies 30 days to confess to furlough fraud - or face big punishments**
<https://www.birminghammail.co.uk/news/midlands-news/government-gives-companies-30-days-18425537>
- **More coronavirus scams reported with vulnerable and disabled at biggest risk of fraud**
<https://www.walesonline.co.uk/news/uk-news/more-coronavirus-scams-reported-vulnerable-18420472>
- **Accessories giant Claire's hacked to steal credit card info**
<https://www.bleepingcomputer.com/news/security/accessories-giant-claires-hacked-to-steal-credit-card-info/>
- **US bank customers targeted in ongoing Qbot campaign**
<https://www.bleepingcomputer.com/news/security/us-bank-customers-targeted-in-ongoing-qbot-campaign/>
- **Nearly a Third of China's 2019 Ad Traffic Found to be Invalid; ByteDance Closes Vigo Apps**
<https://www.exchangewire.com/blog/2020/06/15/nearly-a-third-of-chinas-2019-ad-traffic-found-to-be-invalid-bytedance-closes-vigo-apps/>
- **NYC's contact tracers have been told not to ask people if they've attended a protest**
<https://www.businessinsider.com/nyc-contact-tracers-not-asking-people-attend-george-floyd-protest-2020-6>
- **Ryuk Continues to Dominate Ransomware Response Cases**
<https://www.darkreading.com/vulnerabilities---threats/ryuk-continues-to-dominate-ransomware-response-cases/d/d-id/1338092>
- **Complexity and size of DDoS attacks have increased**
<https://www.helpnetsecurity.com/2020/06/15/2019-ddos-attacks/>
- **Can we safeguard the election infrastructure from cyber attacks?**
<https://www.helpnetsecurity.com/2020/06/15/safeguard-election-infrastructure/>
- **Magecart attackers hit Claire's, Intersport web shops**
<https://www.helpnetsecurity.com/2020/06/15/magecart-claires-intersport/>
- **The FBI expects a surge of mobile banking threats**
<https://www.helpnetsecurity.com/2020/06/15/mobile-banking-threats/>
- **Running ConnectWise Automate on-prem? Fix this high-risk API vulnerability**
<https://www.helpnetsecurity.com/2020/06/15/connectwise-automate-api-vulnerability/>
- **Live Event Manufacturer Reveals Employee Data Breach**
<https://www.infosecurity-magazine.com/news/live-event-manufacturer-employee/>
- **Twitter Shatters 32,000 State-Linked Accounts**
<https://www.infosecurity-magazine.com/news/twitter-shatters-32000-statelinked/>
- **Exposed Cloud Databases Attacked 18 Times Per Day**
<https://www.infosecurity-magazine.com/news/exposed-cloud-databases-attacked/>
- **Poor Password Practices and Growing Acceptance of Biometrics in Financial Accounts**
<https://www.infosecurity-magazine.com/news/password-practices-acceptance/>
- **Foodora Data Breach Impacts Customers in 14 Countries**
<https://www.infosecurity-magazine.com/news/foodora-data-breach/>
- **Mobile Threats Delivered by Adult Content Double**
<https://www.infosecurity-magazine.com/news/mobile-threats-delivered-by-adult/>
- **Protecting Unmanaged & IoT Devices: Why Traditional Security Tools Fail**
<https://threatpost.com/armis-protecting-unmanaged-iot-devices-why-traditional-security-tools-fail/156502/>
- **'Lamphone' Hack Uses Lightbulb Vibrations to Eavesdrop on Homes**
<https://threatpost.com/lamphone-hack-lightbulb-vibrations-eavesdrop/156551/>
- **WFH Alert: Critical Bug Found in Old D-Link Router Models**
<https://threatpost.com/work-from-home-alert-critical-d-link-bug/156573/>

- **Intel Adds Anti-Malware Protection in Tiger Lake CPUs**
<https://threatpost.com/intel-anti-malware-protection-tiger-lake-cpus/156568/>
- **'Vendetta' hackers are posing as Taiwan's CDC in data-theft campaign**
<https://www.cyberscoop.com/vendetta-taiwan-coronavirus-telefonica/>
- **Three years after WannaCry, what have we learned?**
https://www.helpnetsecurity.com/2020/06/15/wannacry-ransomware-lessons/?&web_view=true
- **Does the world need a multilateral cyber hotline?**
https://www.zdnet.com/article/does-the-world-need-a-multilateral-cyber-hotline/?&web_view=true
- **Locked iPhones rendered almost useless in Australia's COVIDSafe tracking efforts**
https://www.zdnet.com/article/locked-iphones-rendered-almost-useless-in-covidsafe-tracking-efforts/?&web_view=true
- **Fraudsters Set Up Shop on the Dark Web Promoting How-To Guides on Filing for Unemployment Benefits**
https://hotforsecurity.bitdefender.com/blog/fraudsters-set-up-shop-on-the-dark-web-promoting-how-to-guides-on-filing-for-unemployment-benefits-23496.html?&web_view=true
- **Accidental Loss of Database Leads to Outage, Potential Threat For Jenkins Artifactory Portal**
<https://cyware.com/news/accidental-loss-of-database-leads-to-outage-potential-threat-for-jenkins-artifactory-portal-11c48407>
- **Gamaredon Hackers Using New Tools for Microsoft Outlook, Office, and Excel**
<https://cyware.com/news/gamaredon-hackers-using-new-tools-for-microsoft-outlook-office-and-excel-63b5f2b9>
- **Check Point: Ursnif Banking Trojan Ranks On Top 10 Malware List for First Time, Over Doubling Its Impact On Organizations**
https://blog.checkpoint.com/2020/06/15/mays-most-wanted-malware-ursnif-banking-trojan-ranks-on-top-10-malware-list-for-first-time-over-doubling-its-impact-on-organizations/?&web_view=true
- **Black Kingdom ransomware operators exploit Pulse VPN flaws**
https://securityaffairs.co/wordpress/104789/cyber-crime/black-kingdom-ransomware-pulse-vpn.html?&web_view=true
- **Dating Apps Exposed 845GB of Explicit Photos, Chats, and More**
https://www.wired.com/story/dating-apps-leak-explicit-photos-screenshots/?&web_view=true
- **Nintendo Accounts Hack: Hackers Playing the Wrong Way**
<https://cyware.com/news/nintendo-accounts-hack-hackers-playing-the-wrong-way-6b8e45d5>
- **Hackers Breached A1 Telekom, Austria's largest ISP**
<https://cyware.com/news/hackers-breached-a1-telekom-austrias-largest-isp-5778d4e9>
- **ARM CPUs Face Threats From New Variant of Spectre Vulnerability**
<https://cyware.com/news/arm-cpus-face-threats-from-new-variant-of-spectre-vulnerability-44250570>
- **Trickbot Malware Spreading Through Fake 'Black Lives Matter' Voting Campaign**
<https://cyware.com/news/trickbot-malware-spreading-through-fake-black-lives-matter-voting-campaign-d9f254de>
- **Scammers Play Trick or Treat Around Coronavirus Through Spamdexing**
<https://cyware.com/news/scammers-play-trick-or-treat-around-coronavirus-through-spamdexing-1b690f7d>

TUESDAY 16th June 2020

- **'All our taps are completely dry': Australian pubs run out of beer after a cyber attack disrupted production at one of the country's biggest breweries**
<https://www.dailymail.co.uk%2Fnews%2Farticle-8426003%2FAustralian-pubs-start-run-beer-cyber-attack-disrupted-production-big-brewery.html&usq=AOvVaw1qUiOuC7JA31rS0jllolI3>
- **Fraud within and against the Commonwealth: The most harmful frauds, 2016-17 to 2018-19**
<http://www.aic.gov.au/publications/sr/sr26>
- **Developing markets in Asia Pacific challenged by ransomware and malware encounters, while developed markets struggle with increased drive-by download attack volumes: Microsoft Security Endpoint Threat Report 2019**
<https://news.microsoft.com/apac/2020/06/16/developing-markets-in-asia-pacific-challenged-by-ransomware-and-malware-encounters-while-developed-markets-struggle-with-increased-drive-by-download-attack-volumes-microsoft-security-endpoint-threat/>
- **Appliance repairer in the dark after ransomware attack on F&P Appliances**
<https://www.stuff.co.nz/business/121849569/appliance-repairer-in-the-dark-after-ransomware-attack-on-fp-appliances>
- **Cyber attack: At least nine rights activists targeted**
<https://www.hindustantimes.com/india-news/cyber-attack-at-least-nine-rights-activists-targeted/story-Z33DVof3JDmslYFyMKW4ol.html>
- **New scam advert alert system launched to target online fraud**
<https://www.itv.com/news/2020-06-16/new-scam-advert-alert-system-launched-to-target-online-fraud/>
- **Federal Bank of India combats card and merchant fraud with support from ACI Worldwide**
<https://www.worldfinanceinforms.com/banking/federal-bank-of-india-combats-card-and-merchant-fraud-with-support-from-aci-worldwide/>
- **Active ransomware campaign leveraging remote access technologies**
<https://www.cert.govt.nz/it-specialists/advisories/active-ransomware-campaign-leveraging-remote-access-technologies/>

- **Banks may need to update policies to fight COVID-19 fraud**
<https://www.reedsmith.com/en/perspectives/2020/06/banks-may-need-to-update-policies-to-fight-covid19-fraud>
- **Harnessing the power of threat intelligence to navigate cybersecurity amidst COVID-19**
<https://news.microsoft.com/apac/2020/06/16/harnessing-the-power-of-threat-intelligence-to-navigate-cybersecurity-amidst-covid-19/>
- **'Covid-19 has highlighted the resource sector's vulnerabilities'**
<https://www.c-resource.com/2020/06/16/covid-19-has-highlighted-the-resource-sectors-vulnerabilities/>
- **Cybersecurity experts on securing the 'new normal' APAC workplace**
<https://techwireasia.com/2020/06/cybersecurity-experts-on-securing-new-normal-apac-workplaces/>
- **COVID-19 themed cyberthreats and attacks on the rise**
<https://www.thailand-business-news.com/tech/79548-covid-19-themed-cyberthreats-and-attacks-on-the-rise.html>
- **Specialist insurer reports 25% ransomware surge in Q1**
<https://www.cybersecasia.net/news/specialist-insurer-reports-25-ransomware-surge-in-q1>
- **Toronto accounting firm hit by ransomware**
<https://business.financialpost.com/technology/tech-news/toronto-accounting-firm-hit-by-ransomware>
- **One-in-five experiences cyber fraud each year**
<https://www.bbc.co.uk/news/uk-scotland-53063418>
- **COVID CLAIMS FRAUD UNDER INVESTIGATION**
[https://www.newLawjournal.co.uk/content/covid-claims-fraud-under-investigation](https://www.newlawjournal.co.uk/content/covid-claims-fraud-under-investigation)
- **Manufacturing ransomware attacks increased 156%**
<https://www.plantservices.com/industrynews/2020/manufacturing-ransomware-attacks-increased-156/>
- **Hackers target Redcar children's charity in attempted cyber attack**
<https://www.gazettelive.co.uk/news/teesside-news/hackers-target-redcar-childrens-charity-18433944>
- **The Government has released a new plan to support cyber security exports**
<https://www.contracts.mod.uk/blog/government-released-new-plan-support-cyber-security-exports/>
- **Vulnerabilities in D-Link router raises concerns over remote worker IT security**
<https://www.scmagazineuk.com/vulnerabilities-d-link-router-raises-concerns-remote-worker-security/article/1686501>
- **Google Alerts catches fake data breach notes pushing malware**
<https://www.bleepingcomputer.com/news/security/google-alerts-catches-fake-data-breach-notes-pushing-malware/>
- **CoinMiner exploits Apple APSDaemon vulnerability to evade detection**
<https://www.bleepingcomputer.com/news/security/coinminer-exploits-apple-apsdaemon-vulnerability-to-evade-detection/>
- **T-Mobile outage caused by fiber circuit failure, not DDoS attacks**
<https://www.bleepingcomputer.com/news/security/t-mobile-outage-caused-by-fiber-circuit-failure-not-ddos-attacks/>
- **Plex fixes Media Server bugs allowing full system takeover**
<https://www.bleepingcomputer.com/news/security/plex-fixes-media-server-bugs-allowing-full-system-takeover/>
- **Coronavirus auto latest: Used car market back to pre-Covid levels in June**
<https://www.verdict.co.uk/motor-finance-online/news/coronavirus-timeline-impact-automotive-industry/>
- **The CIA's massive 'Vault 7' leak resulted from 'woefully lax' security protocols within the agency's own network, an internal report found**
<https://www.businessinsider.com/cia-vault-7-leak-woefully-lax-security-protocol-report-2020-6>
- **IoT Security Trends & Challenges in the Wake of COVID-19**
<https://www.darkreading.com/iot/iot-security-trends-and-challenges-in-the-wake-of-covid-19/a/d-id/1338045>
- **Ransomware from Your Lawyer's Perspective**
<https://www.darkreading.com/endpoint/ransomware-from-your-lawyers-perspective-/a/d-id/1338060>
- **Hosting Provider Hit With Largest-Ever DDoS Attack**
<https://www.darkreading.com/attacks-breaches/hosting-provider-hit-with-largest-ever-ddos-attack/d/d-id/1338107>
- **A look inside privacy enhancing technologies**
<https://www.helpnetsecurity.com/2020/06/16/a-look-inside-privacy-enhancing-technologies/>
- **As IoT devices evolve, risk management needs improvement**
<https://www.helpnetsecurity.com/2020/06/16/iot-risk-management/>
- **Zero-day flaws in widespread TCP/IP library open millions of IoT devices to remote attack**
<https://www.helpnetsecurity.com/2020/06/16/flaws-tcp-ip-library/>
- **Magecart Attackers Target Retail Brands Under Lockdown**
<https://www.infosecurity-magazine.com/news/magecart-attackers-target-retail/>
- **IT Pros Feel #COVID19 Pressure as 66% Cite Increased Security Risks**
<https://www.infosecurity-magazine.com/news/it-pros-feel-covid19-pressure-cite/>
- **46% of SMEs Sharing Confidential Files by Email During Lockdown**
<https://www.infosecurity-magazine.com/news/sme-businesses-sharing/>
- **eBay Executives Charged With Cyber-Stalking Critics**
<https://www.infosecurity-magazine.com/news/ebay-executives-charged-with/>
- **Wiggle Investigates Cyber-Attack**
<https://www.infosecurity-magazine.com/news/wiggle-investigates-cyberattack/>

- **Shadow IT: Why It's Still a Major Risk in Today's Environments**
<https://threatpost.com/forcepoint-shadow-it-why-its-still-a-major-risk-in-todays-environments/156515/>
- **EU member states agree specs for coronavirus app interoperability**
<https://uk.reuters.com/article/us-health-coronavirus-germany-app-europe/eu-member-states-agree-specs-for-coronavirus-app-interoperability-idUKKBN23N1H0>
- **Mass Layoffs Risk Exodus Of Corporate Data, Experts Warn**
<https://www.forbes.com/sites/paulfroberts/2020/06/16/mass-layoffs-risk-exodus-of-corporate-data-experts-warn/#25a9c24e4e12>
- **Survey shows rise in scam robocalls amid COVID-19 fears**
https://www.welivesecurity.com/2020/06/16/survey-how-robocall-scams-prey-covid19-fears/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+eset%2Fblog+%28ESET+Blog%3A+We+Live+Security%29
- **Singapore Rules Out Apple, Google's Contact-Tracing System**
<https://www.bloomberg.com/news/articles/2020-06-15/singapore-rules-out-using-apple-google-contact-tracing-system?srnd=technology-vp>
- **Social Security Wants a New Way to Manage Access for 330 Million Americans**
https://www.nextgov.com/cybersecurity/2020/06/social-security-wants-new-way-manage-access-330-million-americans/166165/?&web_view=true
- **Poor Password Practices and Growing Acceptance of Biometrics in Financial Accounts**
https://www.infosecurity-magazine.com/news/password-practices-acceptance/?&web_view=true
- **Web skimmers found on the websites of Intersport, Claire's, and Icing**
https://www.zdnet.com/article/web-skimmers-found-on-the-websites-of-intersport-claires-and-icing/?&web_view=true
- **Widespread T-Mobile outages cause issues for wireless customers across the US**
https://edition.cnn.com/2020/06/15/business/tmobile-outages-wireless-carriers/index.html?&web_view=true
- **Increased focus on data privacy during pandemic boosts cybersecurity jobs in India: Report**
https://ciso.economictimes.indiatimes.com/news/increased-focus-on-data-privacy-during-pandemic-boosts-cybersecurity-jobs-in-india-report/76397700?&web_view=true
- **XMRig Campaign Target Misconfigured Kubernetes to Mine Cryptocurrency**
<https://cyware.com/news/xmrig-campaign-target-misconfigured-kubernetes-to-mine-cryptocurrency-d7c60403>
- **Snake Ransomware Slithering Across Connected Networks**
<https://cyware.com/news/snake-ransomware-slithering-across-connected-networks-a6fce96b>
- **New collaboration tools and controls have made DoD telework safer**
https://www.c4isrnet.com/it-networks/2020/06/15/new-collaboration-tools-and-controls-have-made-dod-telework-safer/?&web_view=true
- **Hacked: Aussie websites for sale on dark web**
https://www.afr.com/technology/hacked-aussie-websites-for-sale-on-dark-web-20200612-p55227?&web_view=true
- **DarkEyE Evolves Into CloudEyE as a Front For Malware Operations**
<https://cyware.com/news/darkeye-evolves-into-cloudeye-as-a-front-for-malware-operations-7c3001ad>
- **Citizen Lab and Amnesty International Uncover Spyware Operation Against Indian Human Rights Defenders**
https://citizenlab.ca/2020/06/citizen-lab-amnesty-international-uncover-spyware-operation-against-indian-human-rights-defenders/?&web_view=true
- **Zero-day flaws in widespread TCP/IP library open millions of IoT devices to remote attack**
https://www.helpnetsecurity.com/2020/06/16/flaws-tcp-ip-library/?&web_view=true
- **CoinMiner exploits Apple APSDaemon vulnerability to evade detection**
https://www.bleepingcomputer.com/news/security/coinminer-exploits-apple-apsdaemon-vulnerability-to-evade-detection/?&web_view=true
- **Russian Disinfo Operation You Never Heard About**
https://www.wired.com/story/russia-secondary-infektion-disinformation/?&web_view=true
- **BlueJeans announces stronger encryption for video meetings**
https://www.zdnet.com/article/bluejeans-announces-end-to-end-encryption-for-video-meetings/?&web_view=true
- **Oracle E-Business Suite Flaws Let Hackers Hijack Business Operations**
https://thehackernews.com/2020/06/oracle-e-business-suite.html?&web_view=true
- **Sextortionists Using Social Engineering Tactics to Collect Victims' Data**
https://www.tripwire.com/state-of-security/security-data-protection/sextortionists-using-social-engineering-tactics-to-collect-victims-data/?&web_view=true

WEDNESDAY 17th June 2020

- **Eight percent of federal agency resources may be affected by fraud, new research found**
<https://www.themandarin.com.au/135164-eight-percent-of-federal-agency-resources-may-be-affected-by-fraud-new-research-found/>
- **Phishing scams soar in May: ACCC**
<https://www.arnnet.com.au/article/680630/phishing-scams-soar-may-acc/>

- **Cybersecurity: How to stay safe online during COVID-19**
<https://www.ibm.com/blogs/ibm-anz/cybersecurity-how-to-stay-safe-online-during-the-covid-19-pandemic/>
- **Police investigating \$9 million alleged fraud uncover romance scam**
<https://www.smh.com.au/national/nsw/police-investigating-9-million-alleged-fraud-allegedly-uncover-romance-scam-20200617-p553mq.html>
- **WA Bureaucrat Paul Whyte pleads guilty to mammoth fraud scam**
<https://www.theaustralian.com.au/%2Fnation%2Fpolitics%2Fwa-bureaucrat-paul-whyte-pleads-guilty-to-mammoth-fraud-scam%2Fnews-story%2F55955e62050cb199e160257600b129f4&usg=AOvVaw3qax7yoBKq20XW4J0R8539>
- **Chipmaker MaxLinear hit by 'Maze' ransomware attack**
<https://www.itnews.com.au/news/chipmaker-maxlinear-hit-by-maze-ransomware-attack-549341>
- **Microsoft: COVID-19 Cyber Attacks Peaked In March And Fell Off Quickly**
<https://www.forbes.com/sites/leemathews/2020/06/17/microsoft-covid-19-cyber-attacks-peaked-in-march-and-fell-off-quickly/#660c6362c9aa>
- **Increase in investigations arising from fraud tip-off calls to health ministry's Health Integrity Line**
<https://www.nzdoctor.co.nz/article/print-archive/increase-investigations-arising-fraud-tip-calls-health-ministrys-health>
- **CBI Files Rs 67 Crore Bank Fraud Case Against BJP Leader, Four Others**
<https://www.ndtv.com/india-news/cbi-files-rs-67-crore-bank-fraud-case-against-bjp-leader-four-others-2247598>
- **Indian American businessman charged with \$400,000 covid relief fraud**
<https://www.americanbazaaronline.com/2020/06/17/indian-american-businessman-charged-with-400000-covid-relief-fraud-441468/>
- **The rising significance of cybersecurity for logistics**
<https://www.expresscomputer.in/guest-blogs/the-rising-significance-of-cybersecurity-for-logistics/58292/>
- **Ransomware: What it's costing NZ, two killer tips to stop it**
https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12340286
- **The ransomware threat is changing – sectoral implications**
<https://www.dlapiper.com/de/belgium/insights/events/2020/06/the-ransomware-threat-is-changing/17-june-2020/>
- **Honda likely singled out in cyberattack that halted factories**
<https://asia.nikkei.com/Business/Technology/Honda-likely-singled-out-in-cyberattack-that-halted-factories>
- **Hong Kong Recorded All-Time Low Malware and Ransomware Encounters: Microsoft Security Endpoint Threat Report 2019**
<https://news.microsoft.com/en-hk/2020/06/17/hong-kong-recorded-all-time-low-malware-and-ransomware-encounters-microsoft-security-endpoint-threat-report-2019/>
- **Cybercriminals unleash diverse wave of attacks on COVID-19 vaccine researchers**
<https://www.techrepublic.com/article/cybercriminals-unleash-diverse-wave-of-attacks-on-covid-19-vaccine-researchers/>
- **Singapore experienced the highest drive-by download attack volume in Asia Pacific: Microsoft Security Endpoint Threat Report 2019**
<https://news.microsoft.com/en-sg/2020/06/17/singapore-experienced-the-highest-drive-by-download-attack-volume-in-asia-pacific-microsoft-security-endpoint-threat-report-2019/>
- **Cosmetics company Avon offline after cyber attack**
<https://www.computerweekly.com/news/252484804/Cosmetics-company-Avon-offline-after-cyber-attack>
- **Crypto-Ransomware Attacks Are Spreading Like a Hacking Wildfire**
<https://cointelegraph.com/news/crypto-ransomware-attacks-are-spreading-like-a-hacking-wildfire>
- **A View of COVID-19's First Wave of Cybersecurity**
<https://www.infosecurity-magazine.com/blogs/view-covid19-first-wave/>
- **Security threats endanger tens of millions working from home**
<https://securitybrief.eu/story/security-threats-endanger-tens-of-millions-working-from-home>
- **Operation In(ter)ception: Aerospace and military companies in the crosshairs of cyberspies**
<https://www.welivesecurity.com/2020/06/17/operation-interception-aerospace-military-companies-cyberspies/>
- **Trust lacking within the cybercriminal underground: Trend Micro report**
<http://www.hssreview.com/security/trust-lacking-within-the-cybercriminal-underground-trend-micro-report>
- **Fraud reports spiked by nearly 45% in April as scammers take advantage of pandemic**
<https://www.surreynowleader.com/news/fraud-reports-spiked-by-nearly-45-in-april-as-scammers-take-advantage-of-pandemic/>
- **Well-Known Ransomware Gang Strikes Three Companies in the US and Canada**
<https://cointelegraph.com/news/well-known-ransomware-gang-strikes-three-companies-in-the-us-and-canadahttps://cointelegraph.com/news/well-known-ransomware-gang-strikes-three-companies-in-the-us-and-canada>
- **COVID-19 is showing why a vaccine to stop the fraud of EU finances is needed**
<https://www.euronews.com/2020/06/17/covid-19-is-showing-why-a-vaccine-to-stop-the-fraud-of-eu-finances-is-needed-view>
- **'Multistage ransomware attacks are becoming increasingly dangerous'**
<https://www.techzine.eu/news/security/47329/multistage-ransomware-attacks-are-becoming-increasingly-dangerous/>
- **Romanians Behind Cyber-Fraud Ring Plead Guilty in US**
<https://www.riskscreen.com/kyc360/news/romanians-behind-cyber-fraud-ring-plead-guilty-in-us/>

- **More than 100 NHS email addresses hijacked - as city patients warned of 'widespread' cyber-attack**
<https://www.birminghammail.co.uk/news/midlands-news/more-100-nhs-email-addresses-18434073>
- **"Full-on supply chain disaster": Hundreds of millions of IoT devices hit by Ripple20 flaws**
[https://www.scmagazineuk.com/"full-on-supply-chain-disaster"-hundreds-millions-iot-devices-hit-ripple20-flaws/article/1686920](https://www.scmagazineuk.com/)
- **Cyberattackers raising stakes in financial sector, security experts tell House subcommittee**
<https://www.scmagazine.com/home/finance/cyberattackers-raising-stakes-in-financial-sector-security-experts-tell-house-subcommittee/>
- **Bug in 'USB for Remote Desktop' lets hackers add fake devices**
<https://www.bleepingcomputer.com/news/security/bug-in-usb-for-remote-desktop-lets-hackers-add-fake-devices/>
- **New car sales across Europe fall 52% in May**
<https://www.motortrader.com/motor-trader-news/automotive-news/new-car-sales-across-europe-fall-52-may-17-06-2020>
- **China's Great Firewall Looms Over Hong Kong As Surveillance Grows**
<https://www.bloomberg.com/news/articles/2020-06-16/china-s-great-firewall-looms-over-hong-kong-as-surveillance-grows?srnd=technology-vp>
- **Zoom to Offer All Users Full Encryption, Bending to Pressure**
<https://www.bloomberg.com/news/articles/2020-06-17/zoom-to-offer-free-users-full-encryption-bending-to-pressure?srnd=technology-vp>
- **Kim Jong Un has quietly built a 7,000-man cyber army that gives North Korea an edge nuclear weapons don't**
<https://www.businessinsider.com/north-korea-kim-jong-un-cyber-army-cyberattacks-nuclear-weapons-2020-6>
- **BEC Attacks on the C-Suite Dropped 37% in Q1**
<https://www.darkreading.com/attacks-breaches/bec-attacks-on-the-c-suite-dropped-37--in-q1/d/d-id/1338105>
- **Work from home, work from anywhere: Are you secure everywhere?**
<https://www.helpnetsecurity.com/2020/06/17/work-from-home-security/>
- **Cybercriminals banking on finance: Mitigating escalation**
<https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/>
- **#COVID19 Forces Positive Long-Term Changes to Cybersecurity**
<https://www.infosecurity-magazine.com/news/covid19-forces-positive-longterm/>
- **Illinois Tech CEO Charged with #COVID19 Relief Fraud**
<https://www.infosecurity-magazine.com/news/illinois-tech-ceo-charged-with/>
- **Sharp Rise in Web Attacks on Gamers**
<https://www.infosecurity-magazine.com/news/sharp-rise-in-web-attacks-on-gamers/>
- **Fighting Cyber Attacks with Game Theory**
<https://threatpost.com/trapx-fighting-cyber-attacks-with-game-theory/156545/>
- **Premier League's Return: A Hat Trick of Cyberthreats?**
<https://threatpost.com/premier-leagues-return-hat-trick-of-cyberthreats/156684/>
- **AcidBox Malware Uncovered Using Repurposed VirtualBox Exploit**
<https://threatpost.com/acidbox-malware-uncovered-using-repurposed-virtualbox-exploit/156653/>
- **Serco boss defends its work on setting up NHS test-and-trace system**
<https://www.theguardian.com/business/2020/jun/17/serco-boss-defends-its-work-on-setting-up-nhs-test-and-trace-system-coronavirus>
- **Akamai Discloses Details of Massive DDoS Attack**
<https://securityboulevard.com/2020/06/akamai-discloses-details-of-massive-ddos-attack/>
- **More ad fraud apps found hiding on Google Play Store**
<https://nakedsecurity.sophos.com/2020/06/17/more-ad-fraud-apps-found-hiding-on-google-play-store/>
- **New U.S. pandemic watchdog says data, tech issues challenge oversight work**
<https://uk.reuters.com/article/us-health-coronavirus-usa-fraud/new-u-s-pandemic-watchdog-says-data-tech-issues-challenge-oversight-work-idUKKBN23O2D2>
- **French watchdog warns against COVID-19 smart surveillance**
<https://uk.reuters.com/article/us-health-coronavirus-france-privacy/french-watchdog-warns-against-covid-19-smart-surveillance-idUKKBN23O2T7>
- **VLC Media Player 3.0.11 fixes severe remote code execution flaw**
https://www.bleepingcomputer.com/news/security/vlc-media-player-3011-fixes-severe-remote-code-execution-flaw/?&web_view=true
- **DraftKings discloses SBTech ransomware attack in SEC filing**
https://www.bleepingcomputer.com/news/security/draftkings-discloses-sbtech-ransomware-attack-in-sec-filing/?&web_view=true
- **Adobe Patches 18 Critical Flaws in Out-Of-Band Update**
https://threatpost.com/adobe-patches-18-critical-flaws-in-out-of-band-update/156609/?&web_view=true
- **Researchers find abuse of cloud platforms by hackers and security professionals alike**
https://www.theregister.com/2020/06/17/cloud_services_hacking/?&web_view=true

- **30,000+ Italian sales agents' personal data, IDs leaked by MLM company that distributes wellness products**
https://cybernews.com/security/italian-sales-agents-personal-data-leaked-by-mlm-company/?&web_view=true
- **North Korea's state hackers caught engaging in BEC scams**
https://www.zdnet.com/article/north-koreas-state-hackers-caught-engaging-in-bec-scams/?&web_view=true
- **Amnesty Sounds Alarm Over Gulf, Norway Virus Apps**
https://www.securityweek.com/amnesty-sounds-alarm-over-gulf-norway-virus-apps?&web_view=true
- **Now, Contact-Tracing Apps Are on the Radar of Hackers**
<https://cyware.com/news/now-contact-tracing-apps-are-on-the-radar-of-hackers-808f895b>
- **Android Apps can be Hacked by Exploiting its Internal Messaging Components**
<https://cyware.com/news/android-apps-can-be-hacked-by-exploiting-its-internal-messaging-components-0fa4d0cd>
- **Cybercriminals banking on finance: Mitigating escalation**
https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/?web_view=true
- **What is Going on with Elasticsearch?**
<https://cyware.com/news/what-is-going-on-with-elasticsearch-439f8d19>
- **#COVID19 Forces Positive Long-Term Changes to Cybersecurity**
https://www.infosecurity-magazine.com/news/covid19-forces-positive-longterm/?&web_view=true
- **Magecart Scammers Exploit the Pandemic to Stretch Their Attack Surface**
<https://cyware.com/news/magecart-scammers-exploit-the-pandemic-to-strech-their-attack-surface-8d47b2c1>
- **Here are the states hit hardest by coronavirus scams**
https://www.cnn.com/2020/06/16/states-hit-hardest-by-coronavirus-scams.html?&web_view=true
- **Singapore experienced the highest drive-by download attack volume in Asia Pacific**
https://news.microsoft.com/en-sg/2020/06/17/singapore-experienced-the-highest-drive-by-download-attack-volume-in-asia-pacific-microsoft-security-endpoint-threat-report-2019/?&web_view=true
- **Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals**
https://home.treasury.gov/news/press-releases/sm1034?&web_view=true
- **NCSC Warns Football Fans of Potential Scams**
https://www.zdnet.com/article/phishing-warning-reset-your-password-to-lockout-crooks-football-fans-told/?&web_view=true
- **Technology has inevitably changed the cyber space game**
https://www.itweb.co.za/content/j5alrMQaGKnMpYQk?&web_view=true
- **Cybercrime And Cryptocurrency Exchange Hacks Up By 75% During Coronavirus Pandemic, FBI Reveals**
https://www.ibtimes.com/cybercrime-cryptocurrency-exchange-hacks-75-during-coronavirus-pandemic-fbi-reveals-2995527?&web_view=true
- **Digital banking in Indonesia prioritises security amid cyber threats**
https://www.thestar.com.my/aseanplus/aseanplus-news/2020/06/17/digital-banking-in-indonesia-prioritises-security-amid-cyber-threats?&web_view=true
- **Cybersecurity Index Shows the Most Exposed Countries**
https://www.securitymagazine.com/articles/92614-cybersecurity-index-shows-the-most-exposed-countries?&web_view=true

THURSDAY 18th June 2020

- **Potential cost of fraud against govt \$1.7 billion**
<https://www.governmentnews.com.au/potential-cost-of-govt-fraud-put-at-1-7-billion/https://www.governmentnews.com.au/potential-cost-of-govt-fraud-put-at-1-7-billion/>
- **Half of Security Professionals Had No Contingency Plan in Place for COVID-19**
<https://uktechnews.co.uk/2020/06/18/half-of-security-professionals-had-no-contingency-plan-in-place-for-covid-19/>
- **China opens another front, steps up cyberattacks that target India: Intel**
<https://www.hindustantimes.com/india-news/china-steps-up-cyberattacks-intel/story-hQXYHWJTtRq1ut6P0g7yGL.html>
- **Massive spying on users of Google's Chrome shows new security weakness**
https://economictimes.indiatimes.com/tech/internet/massive-spying-on-users-of-googles-chrome-shows-new-security-weakness/articleshow/76438320.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **India-China Standoff Impact Spills Over To Telecom Sector, Cybersecurity Concerns**
<https://inc42.com/buzz/india-china-standoff-impact-spills-over-to-telecom-sector-cybersecurity-concerns/>
- **How a T-Mobile Outage Got Mistaken for a Cyber Attack**
<https://www.bloombergquint.com/gadfly/fcc-shouldn-t-let-t-mobile-outage-be-mistaken-for-cyber-attack>
- **Amazon 'thwarts largest ever DDoS cyber-attack'**
<https://www.bbc.co.uk/news/technology-53093611>
- **CERT NZ Releases Advisory on Ransomware Campaign**
<https://www.us-cert.gov/ncas/current-activity/2020/06/18/cert-nz-releases-advisory-ransomware-campaign>
- **In IT security, 'good enough' is no longer good enough**
<https://securitybrief.eu/story/in-it-security-good-enough-is-no-longer-good-enough>

- **Ransomware group threatens to 'auction' confidential Lion files if \$1.25m ransom not paid**
<https://www.stuff.co.nz/business/121856473/calls-grow-for-government-action-after-lion-receives-us800000-ransomware-demand>
- **China launches cyber attacks on government websites and banks following India MASSACRE**
<https://www.express.co.uk/news/world/1297502/China-cyber-attacks-India-government-targets-border-deaths-world-war-3>
- **Covid-19 Relief: North Korea Hackers Lazarus Planning Massive Attack on US, UK, Japan, Singapore, India, South Korea?**
<https://www.databreaches.net/covid-19-relief-north-korea-hackers-lazarus-planning-massive-attack-on-us-uk-japan-singapore-india-south-korea/>
- **CISA Warns of Ongoing Ransomware Campaign Exploiting Vulnerabilities in RDP and VPNs**
<https://www.hipaajournal.com/cisa-warns-of-ongoing-ransomware-campaign-exploiting-vulnerabilities-in-rdp-and-vpns/>
- **BlackBerry and Intel partner to stop cryptojacking malware**
<https://cyberriskleaders.com/blackberry-and-intel-partner-to-stop-cryptojacking-malware/>
- **Middle East Cybersecurity Market Worth \$29.9 Bn Post COVID-19**
<https://www.cisomag.com/middle-east-cybersecurity-market-worth-29-9-bn-post-covid-19/>
- **UK FM claims that Russia and China seek to exploit COVID-19 pandemic**
https://iranpress.com/europe-i148635-uk_fm_claims_that_russia_and_china_seek_to_exploit_covid_19_pandemic
- **Half of Mobile Banking Apps are Vulnerable to Fraud Data Theft**
<https://www.cisomag.com/flaws-in-mobile-banking-apps/>
- **Canada a target for cyberattacks on COVID-19 research**
<https://www.theglobeandmail.com/featured-reports/article-canada-a-target-for-cyberattacks-on-covid-19-research/>
- **Former Stevens Point hotel owner gets 87 months in federal prison for identity theft, wire fraud**
<https://eu.stevenspointjournal.com/story/news/2020/06/18/stevens-point-crime-ex-hotel-owner-sentenced-id-theft-wire-fraud/3218420001/>
- **Management of six hotels operating in Georgia found to be involved in large-scale fraud**
<https://agenda.ge/en/news/2020/1930>
- **Much-needed unemployment benefits still on hold as state's fraud investigation continues**
<https://www.boston25news.com/news/25-investigates/much-needed-unemployment-benefits-still-hold-states-fraud-investigation-continues/XYUHKEUDJRG5VQBQ75I7XE2ZYWY/>
- **Bounce Back loans to keep small businesses afloat in the coronavirus crisis are being splashed out on supercars, motor industry insiders claim**
<https://www.thisismoney.co.uk/money/cars/article-8436599/Bounce-Loans-splashed-supercars-insiders-claim.html>
- **Malicious Google extensions research points out 'unintended consequence' of cloud computing**
<https://www.scmagazine.com/home/security-news/malicious-google-extensions-research-points-out-unintended-consequence-of-cloud-computing/>
- **InvisiMole malware delivered by Gamaredon hacker group**
<https://www.bleepingcomputer.com/news/security/invisimole-malware-delivered-by-gamaredon-hacker-group/>
- **Why did this Bank of America phishing email bypass spam filters?**
<https://www.bleepingcomputer.com/news/security/why-did-this-bank-of-america-phishing-email-bypass-spam-filters/>
- **New Cisco Webex Meetings flaw lets attackers steal auth tokens**
<https://www.bleepingcomputer.com/news/security/new-cisco-webex-meetings-flaw-lets-attackers-steal-auth-tokens/>
- **Hijacked Oxford server used by hackers for Office 365 phishing**
<https://www.bleepingcomputer.com/news/security/hijacked-oxford-server-used-by-hackers-for-office-365-phishing/>
- **79 Netgear router models risk full takeover due to unpatched bug**
<https://www.bleepingcomputer.com/news/security/79-netgear-router-models-risk-full-takeover-due-to-unpatched-bug/>
- **Wells Fargo phishing baits customers with calendar invites**
<https://www.bleepingcomputer.com/news/security/wells-fargo-phishing-baits-customers-with-calendar-invites/>
- **Fight government surveillance during COVID with this VPN**
<https://www.bleepingcomputer.com/offer/deals/fight-government-surveillance-during-covid-with-this-vpn/>
- **Auction numbers up 135% month-on-month, says Dealer Auction**
<https://www.motortrader.com/motor-trader-news/automotive-news/auction-numbers-135-month-month-says-dealer-auction-18-06-2020>
- **Mastercard and Visa face payout following Supreme Court ruling**
<https://www.motortrader.com/motor-trader-news/automotive-news/mastercard-visa-face-payout-dealers-following-supreme-court-ruling-18-06-2020>
- **Hackers tied to North Korea used LinkedIn to break into European defense firms by offering employees fake jobs**
<https://www.businessinsider.com/cyber-spies-use-linkedin-to-hack-european-defence-firms-2020-6>
- **Healthcare CISOs Share COVID-19 Response Stories**
<https://www.darkreading.com/threat-intelligence/healthcare-cisos-share-covid-19-response-stories/d/d-id/1338132>
- **60% of Businesses Plan to Spend More on Cyber Insurance**
<https://www.darkreading.com/risk/60--of-businesses-plan-to-spend-more-on-cyber-insurance/d/d-id/1338127>

- **The Pentagon says it needs to be ready should an adversary try to fry satellites by detonating a nuke in space**
<https://www.businessinsider.com/pentagon-worried-nuke-detonation-in-space-could-fry-satellites-2020-6>
- **Facebook Files Suits to Block Unauthorized Automation Software**
<https://www.bloomberg.com/news/articles/2020-06-18/facebook-files-suits-to-block-unauthorized-automation-software-kbkyksve?smd=technology-vp>
- **Most Contact-Tracing Apps Fail Basic Security**
<https://www.darkreading.com/application-security/most-contact-tracing-apps-fail-basic-security/d/d-id/1338122>
- **83% of Global 2000 enterprises have not adopted basic domain security practices**
<https://www.helpnetsecurity.com/2020/06/18/enterprise-domain-security-practices/>
- **PCI SSC updates standard for payment devices to protect cardholder data**
<https://www.helpnetsecurity.com/2020/06/18/pts-poi-standard/>
- **Email security challenges and BEC trends during the pandemic**
<https://www.helpnetsecurity.com/2020/06/18/email-security-challenges-2020/>
- **#COVID19 Attacks Still Less Than 2% of Total Threats**
<https://www.infosecurity-magazine.com/news/covid19-attacks-less-than-2-total/>
- **Pandemic Popularity Forces Dark Web Forums to Recruit**
<https://www.infosecurity-magazine.com/news/pandemic-popularity-dark-web/>
- **ICO Report Calls for Reforms Around Police Data Extraction**
<https://www.infosecurity-magazine.com/news/ico-police-data-exfiltration/>
- **UK U-Turns on Contact Tracing App Privacy**
<https://www.infosecurity-magazine.com/news/uk-uturns-on-contact-tracing-app/>
- **FCC Warned Against Approving US/Hong Kong Subsea Cable**
<https://www.infosecurity-magazine.com/news/fcc-warned-against-approving-plcn/>
- **ESET Reveals New Insights into Espionage Group InvisiMole**
<https://www.infosecurity-magazine.com/news/eset-insights-cyber-espionage/>
- **US Indicts Six Nigerians Over \$6m Email Scam**
<https://www.infosecurity-magazine.com/news/us-indicts-6-nigerians-over-6m/>
- **Phishing Campaign Targeting Office 365, Exploits Brand Names**
<https://threatpost.com/phishing-campaign-targeting-office-365-exploits-brand-names/156698/>
- **Five Password Tips for Securing the New WFH Normal**
<https://threatpost.com/specops-five-password-tips-for-securing-the-new-wfh-normal/156590/>
- **IcedID Banker is Back, Adding Steganography, COVID-19 Theme**
<https://threatpost.com/icedid-banker-adding-steganography-covid-19-theme/156718/>
- **Piloted in May, ditched in June: the failure of England's Covid-19 app**
<https://www.theguardian.com/world/2020/jun/18/piloted-in-may-ditched-in-june-the-failure-of-englands-covid-19-app>
- **Employees' Reasons for Not Using Secure Communications**
<https://securityboulevard.com/2020/06/employees-reasons-for-not-using-secure-communications/>
- **Bundlore adware brings a new nest of risks to Mac users**
<https://nakedsecurity.sophos.com/2020/06/18/bundlore-adware-brings-a-new-nest-of-risks-to-mac-users/>
- **Security Cameras May Cause Security Troubles Due To These Serious Vulnerabilities**
<https://cyware.com/news/security-cameras-may-cause-security-troubles-due-to-these-serious-vulnerabilities-77dfd694>
- **Feds, states unveil pilot program meant to secure voter databases and other election systems**
https://www.cyberscoop.com/election-security-pilot-voter-databases-cis/?&web_view=true
- **Multi-stage APT attack drops Cobalt Strike using Malleable C2 feature**
https://blog.malwarebytes.com/threat-analysis/2020/06/multi-stage-apt-attack-drops-cobalt-strike-using-malleable-c2-feature/?&web_view=true
- **Ghosts From the Past: Flaws in Legacy GTP Protocol to Impact Future 5G Networks**
<https://cyware.com/news/ghosts-from-the-past-flaws-in-legacy-gtp-protocol-to-impact-future-5g-networks-d5762c26>
- **Business Associate Incidents Added to Breach Tally**
https://www.govinfosecurity.com/business-associate-incidents-added-to-breach-tally-a-14456?&web_view=true
- **Revisiting Ryuk: The Very Busy Ransomware Family**
<https://cyware.com/news/revisiting-ryuk-the-very-busy-ransomware-family-9950406f>
- **Because IT security and the C-suite are misaligned, digital transformation increases cyber risk**
https://www.helpnetsecurity.com/2020/06/18/digital-transformation-cyber-risk/?&web_view=true
- **When Security Takes a Backseat to Productivity**
https://krebsonsecurity.com/2020/06/when-security-takes-a-backseat-to-productivity/?&web_view=true
- **Shlayer Mac Malware Returns with Extra Sneakiness**
https://threatpost.com/shlayer-mac-malware-extra-sneakiness/156669/?&web_view=true
- **Keizer city computers hacked**
https://www.keizertimes.com/posts/1639/keizer-city-computers-hacked?&web_view=true
- **IoT Alliance Australia Developing New 'Trust Mark' Certification for IoT Devices**
https://www.bankinfosecurity.com/australia-developing-trust-mark-for-connected-devices-a-14459?&web_view=true

- **Japan urges citizens to install virus-tracking app, experts echo privacy concerns**
https://ciso.economictimes.indiatimes.com/news/japan-urges-citizens-to-install-virus-tracking-app/76443206?&web_view=true
- **Labor asks for the whereabouts of Australia's overdue cybersecurity strategy**
https://www.zdnet.com/article/labor-asks-for-the-whereabouts-of-australias-overdue-cybersecurity-strategy/?&web_view=true
- **Unemployment Benefit Fraud Runs Rampant in the U.S. as Dark Web Boasts of Stolen Records**
<https://cyware.com/news/unemployment-benefit-fraud-runs-rampant-in-the-us-as-dark-web-boasts-of-stolen-records-3dff645f>
- **Clipper Malware Operators Now Use Cloned Sites to Lure Victims**
<https://cyware.com/news/clipper-malware-operators-now-use-cloned-sites-to-lure-victims-111b5ede>
- **Revised DOJ compliance guidance offers risk-management lessons for cybersecurity leaders**
https://www.csoonline.com/article/3563017/revised-doj-compliance-guidance-offers-risk-management-lessons-for-cybersecurity-leaders.html?&web_view=true
- **Pulse Secure VPN Vulnerabilities Leveraged by Black Kingdom Ransomware**
<https://cyware.com/news/pulse-secure-vpn-vulnerabilities-leveraged-by-black-kingdom-ransomware-aa0e1ed8>
- **Ginp Malware Operations are on the Rise with Expansions in Turkey**
https://securityintelligence.com/posts/ginp-malware-operations-rising-expansions-turkey/?&web_view=true
- **The Largest Ever DDoS Attack**
<https://cyware.com/news/the-largest-ever-ddos-attack-89b5996b>
- **Et tu, LinkedIn? Unfolding a New Technique of Spear-Phishing**
<https://cyware.com/news/et-tu-linkedin-unfolding-a-new-technique-of-spear-phishing-c8bda3f3>
- **TWO PRINT SHOPS PRODUCING FAKE EU DOCUMENTS DISMANTLED IN PARIS**
<https://www.europol.europa.eu/newsroom/news/two-print-shops-producing-fake-eu-documents-dismantled-in-paris>

FRIDAY 19th June 2020

- **China is blamed for huge cyber attack on Australian businesses, schools and hospitals amid increasing war of words between Canberra and Beijing over calls for international inquiry into COVID-19**
<https://www.dailymail.co.uk/news/article-8438205/Huge-cyber-attack-aimed-Australian-government.html>
- **Coronavirus Australia update: China denies it is behind 'major' cyber attacks announced by PM**
<https://www.theguardian.com/australia-news/live/2020/jun/19/australia-coronavirus-latest-updates-coalition-welfare-victoria-community-transmission-scott-morrison-borders-tourism-live-news>
- **Coronavirus timeline: how has it affected financial services?**
<https://www.verdict.co.uk/retail-banker-international/news/coronavirus-timeline-financial-services/>
- **Under Attack: Lion Suffers Second Cyberattack and the Federal Government Warns of an Active Cyberattack on Australian Organisations**
<https://www.natlawreview.com/article/under-attack-lion-suffers-second-cyberattack-and-federal-government-warns-active>
- **Five Eyes alliance agrees to work together to combat Covid-19 cyber attacks**
<https://tech.newstatesman.com/security/five-eyes-alliance-covid-19-cyber-attacks>
- **Cybersecurity, the Covid World, and a Brand New Local Authority**
<https://www.cbronline.com/opinion/buckinghamshire-council-managed-cybersecurity-council>
- **KUDANKULAM MALWARE ATTACK**
<https://economictimes.indiatimes.com/topic/kudankulam-malware-attack>
- **Cyber Attacks Targeting Gamers Witnesses Spike of 54% During Covid-19 Lockdown**
<https://www.news18.com/news/tech/cyber-attacks-targeting-gamers-witnesses-spike-of-54-during-covid-19-lockdown-2676885.html>
- **Wirecard says it cannot rule out 'fraud of considerable proportions'**
<http://www.journalpioneer.com/business/reuters/wirecard-says-it-cannot-rule-out-fraud-of-considerable-proportions-464007/>
- **Indian national jailed in Singapore for GST fraud**
<https://www.wionews.com/india-news/indian-national-jailed-in-singapore-for-gst-fraud-307083>
- **DHS Alerts to Ransomware Campaign Targeting Remote Access Systems**
<https://healthitsecurity.com/news/dhs-alerts-to-ransomware-campaign-targeting-remote-access-systems>
- **Developing APAC remained hotbed of ransomware, malware attacks in 2019**
<https://www.frontier-enterprise.com/developing-apac-remained-hotbed-of-ransomware-malware-attacks-in-2019/>
- **COVID-19 impact: Indian firms see six-fold rise in ransomware attacks**
<https://www.moneycontrol.com/news/business/covid-19-impact-indian-firms-see-six-fold-rise-in-ransomware-attacks-5430011.html>
- **Maze ransomware attack: Names, account numbers of company credit cards compromised, says Cognizant**
<https://www.moneycontrol.com/news/business/maze-ransomware-attack-names-account-numbers-of-company-credit-cards-compromised-says-cognizant-5430611.html>

- **Online shopping fraud hits £16m during lockdown**
<https://www.computerweekly.com/news/252484920/Online-shopping-fraud-hits-16m-during-lockdown>
- **Isolationist approach leaves UK firms exposed to cyber-threats**
<https://www.consultancy.uk/news/24872/isolationist-approach-leaves-uk-firms-exposed-to-cyber-threats>
- **Phishing becoming more prolific and impregnable - report**
<https://securitybrief.eu/story/phishing-becoming-more-prolific-and-impregnable-report>
- **Artificial Intelligence (AI) in Cybersecurity Market Worth \$46.3 billion by 2027- Exclusive Report Covering Pre and Post COVID-19 Market Estimates by Meticulous Research®**
<https://www.globenewswire.com/news-release/2020/06/19/2050757/0/en/Artificial-Intelligence-AI-in-Cybersecurity-Market-Worth-46-3-billion-by-2027-Exclusive-Report-Covering-Pre-and-Post-COVID-19-Market-Estimates-by-Meticulous-Research.html>
- **Government warns against major upcoming phishing attack which promises free Covid-19 testing**
https://economictimes.indiatimes.com/tech/ites/indian-govt-warns-against-major-upcoming-phishing-attack-which-promises-free-covid-19-testing/articleshow/76469119.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **COVID-19 crisis is a potential geopolitical game-changer, warn MEPs**
<https://www.wired-gov.net/wg/news.nsf/articles/COVID19+crisis+is+a+potential+geopolitical+gamechanger+warn+MEPs+19062020123800?open>
- **CORONA Impact on Fraud Detection and Prevention (FDP) Market Growing at a CAGR 28.4% | Key Player IBM, FICO, SAS, BAE, SAP**
<https://www.newschannelnebraska.com/story/42269104/corona-impact-on-fraud-detection-and-prevention-fdp-market-growing-at-a-cagr-284-key-player-ibm-fico-sas-bae-sap>
- **Cyber attacks use LinkedIn to target companies and employees**
<https://securitybrief.eu/story/cyber-attacks-use-linkedin-to-target-companies-and-employees>
- **Phishing attack exploited Samsung, Adobe servers for Office 365 credentials**
<https://securitybrief.eu/story/phishing-attack-exploited-samsung-adobe-servers-for-office-365-credentials>
- **U.S. accuses five Canadians of running \$25M COVID-19 pump-and-dump stock market swindle**
<https://nationalpost.com/news/u-s-accuses-five-canadians-of-running-25m-covid-19-stock-market-swindle>
- **Cryptocurrency ransomware is spreading like wildfire**
<https://www.europeworldnews.com/cryptocurrency-ransomware-is-spreading-like-wildfire/>
- **7 Plead Not Guilty to Looting More than \$132 Million from South African Bank**
<https://www.voanews.com/africa/7-plead-not-guilty-looting-more-132-million-south-african-bank>
- **More than a third of furloughed staff pressured to keep working, survey finds**
<https://cardealermagazine.co.uk/publish/third-furloughed-staff-pressured-keep-working-survey-finds/195762>
- **23 CHARGED IN AUTO DEALER FRAUD NETWORK; 'DEALERS' FREQUENTED LANCASTER COUNTY AUCTION SITES**
<https://lancaster.crimewatchpa.com/da/11617/post/23-charged-auto-dealer-fraud-network-dealers-frequented-lancaster-county-auction-sites>
- **Criminal investigation into cyber attack on council remains 'live'**
<https://www.gazettelive.co.uk/news/teesside-news/criminal-investigation-cyber-attack-council-18446364>
- **Scam warning over NHS coronavirus Test and Trace service**
<https://www.msn.com/en-gb/news/newslondon/scam-warning-over-nhs-coronavirus-test-and-trace-service/ar-BB15KqFW?ocid=spartan-ntp-feeds>
- **Report: Lazarus Group has large-scale Covid-19 phishing campaign in the works**
<https://www.scmagazine.com/home/security-news/news-archive/coronavirus/report-lazarus-group-has-large-scale-covid-19-phishing-campaign-in-the-works/>
- **NetWalker claims credit for attack on Crozer-Keystone Health System**
<https://www.scmagazine.com/home/health-care/netwalker-claims-credit-for-attack-on-crozer-keystone-health-system/>
- **Hackers use fake Windows error logs to hide malicious payload**
<https://www.bleepingcomputer.com/news/security/hackers-use-fake-windows-error-logs-to-hide-malicious-payload/>
- **Nigerian entrepreneur pleaded guilty to \$11M Caterpillar fraud**
<https://www.bleepingcomputer.com/news/security/nigerian-entrepreneur-pleaded-guilty-to-11m-caterpillar-fraud/>
- **Small business directors are spending Bounce Back Loan cash on new luxury cars for themselves, say dealers**
<https://cardealermagazine.co.uk/publish/small-business-directors-spending-bounce-back-loan-cash-new-luxury-cars-report-car-dealers/195760>
- **Apple 'not told' about UK's latest app plans**
https://www.bbc.co.uk/news/technology-53105642?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **UK tells telcos to stockpile Huawei gear in face of U.S. sanctions: letter**
<https://www.businessinsider.com/uk-tells-telcos-to-stockpile-huawei-gear-in-face-of-us-sanctions-letter-2020-6?r=US&IR=T>

- **Pompeo: China uses disinformation to split Europe, US**
<https://www.businessinsider.com/pompeo-china-uses-disinformation-to-split-europe-us-2020-6?r=US&IR=T>
- **Most COVID-19 contact-tracing apps are not adequately secured**
<https://www.helpnetsecurity.com/2020/06/18/contact-tracing-apps-security/>
- **Vulnerable platform used in power plants enables attackers to run malicious code on user browsers**
<https://www.helpnetsecurity.com/2020/06/18/icsa-20-163-01/>
- **Australian cyber attack: Which countries would do it?**
https://www.bbc.co.uk/news/av/world-australia-53102997/australian-cyber-attack-which-countries-would-do-it?intlink_from_url=https%3A%2F%2Fwww.bbc.co.uk%2Fnews%2Ftopics%2Fcz4pr2qd85qt%2Fcyber-security&link_location=live-reporting-map
- **Using Cisco Webex for your video conferencing needs? Go patch!**
<https://www.helpnetsecurity.com/2020/06/18/using-cisco-webex-for-your-video-conferencing-needs-go-patch/>
- **How much is your data worth on the dark web?**
<https://www.helpnetsecurity.com/2020/06/19/dark-web-prices/>
- **How the pandemic affected DDoS attack patterns, global internet traffic**
<https://www.helpnetsecurity.com/2020/06/19/internet-traffic-patterns-ddos/>
- **Drupal fixes three vulnerabilities, including one RCE**
<https://www.helpnetsecurity.com/2020/06/19/cve-2020-13663/>
- **Malicious Chrome Extensions Downloaded Over 33 Million Times**
<https://www.infosecurity-magazine.com/news/malicious-chrome-extensions/>
- **US Deports NeverQuest Cyber-Thief**
<https://www.infosecurity-magazine.com/news/us-deports-neverquest-cyberthief/>
- **FEMA Employee Indicted for Hacking Medical Center**
<https://www.infosecurity-magazine.com/news/fema-employee-indicted-for-hacking/>
- **Former DIA Analyst Sentenced to Prison Over Data Leak**
<https://threatpost.com/former-dia-analyst-sentenced-to-prison-over-data-leak/156775/>
- **NHS Covid app developers 'tried to block rival symptom trackers'**
<https://www.theguardian.com/technology/2020/jun/20/nhs-covid-app-developers-tried-to-block-rival-symptom-trackers>
- **Why the NHS Covid-19 contact tracing app failed**
<https://www.wired.co.uk/article/nhs-tracing-app-scrapped-apple-google-uk>
- **Yes, Apple And Google Have Given Us A Serious Contact Tracing Problem—Here's Why**
<https://www.forbes.com/sites/zakdoffman/2020/06/19/how-apple-and-google-created-this-contact-tracing-disaster/#62a289097ca2>
- **FBI uses T-shirt, tattoo and Vimeo clips to track down alleged arsonist**
<https://nakedsecurity.sophos.com/2020/06/19/fbi-uses-t-shirt-tattoo-and-vimeo-clips-to-track-down-alleged-arsonist/>
- **IBM Maximo Asset Management servers patched against attacks**
<https://nakedsecurity.sophos.com/2020/06/19/ibm-maximo-asset-management-servers-patched-against-attacks/>
- **The smaller the business, the smaller the focus on cybersecurity**
https://www.helpnetsecurity.com/2020/06/19/small-business-cybersecurity/?&web_view=true
- **Google removes 106 Chrome extensions for collecting sensitive user data**
https://www.zdnet.com/article/google-removes-106-chrome-extensions-for-collecting-sensitive-user-data/?&web_view=true
- **NSA Piloting Secure Domain Name System Service for Defense Contractors**
https://www.nextgov.com/cybersecurity/2020/06/nsa-piloting-secure-domain-name-system-service-defense-contractors/166248/?&web_view=true
- **Maze Ransomware Gang Continues Data-Leaking Spree**
https://www.govinfosecurity.com/blogs/maze-ransomware-gang-continues-data-leaking-spree-p-2908?&web_view=true
- **Four zero-days spotted in attacks on honeypot systems**
https://www.zdnet.com/article/security-four-zero-day-attacks-spotted-in-attacks-against-honeypot-systems/?&web_view=true
- **North Korean state hackers reportedly planning COVID-19 phishing campaign targeting 5M across six nations**
https://www.zdnet.com/article/north-korean-state-hackers-reportedly-planning-covid-19-phishing-campaign-targeting-5m-across-six-nations/?&web_view=true
- **Intel agencies alert Railways about malware attack in its system**
https://ciso.economicstimes.indiatimes.com/news/intel-agencies-alert-railways-about-malware-attack-in-its-system/76464257?&web_view=true
- **NSA Revises Guidance on Teleworking Services for Government Users**
https://www.nextgov.com/cybersecurity/2020/06/nsa-revises-guidance-teleworking-services-government-users/166266/?&web_view=true
- **Microsoft Defender ATP now scans Windows 10 PC firmware for hardware rootkit attacks**
https://www.zdnet.com/article/microsoft-defender-atp-now-scans-windows-10-pc-firmware-for-hardware-rootkit-attacks/?&web_view=true

- **Elon Musk Bitcoin vanity addresses used to scam users out of \$2 million**
https://www.zdnet.com/article/elon-musk-bitcoin-vanity-addresses-used-to-scam-users-out-of-2-million/?&web_view=true
 - **Philadelphia-area health system says it 'isolated' a malware attack**
https://www.cyberscoop.com/crozer-keystone-cyber-attack-netwalker-ransomware/?&web_view=true
 - **EXPLOITING ISOLATION: SEXUAL PREDATORS INCREASINGLY TARGETING CHILDREN DURING COVID PANDEMIC**
<https://www.europol.europa.eu/newsroom/news/exploiting-isolation-sexual-predators-increasingly-targeting-children-during-covid-pandemic>
- [End]

The contents of this report are all taken from 3rd party sources and PROFIT does not endorse or warrant the information as being accurate or correct. The sources referred to are either well known specialist IT industry websites or general press websites however we cannot guarantee the links or websites as being malware free.

PROFIT is the working name of Prevention of Fraud in Travel Ltd a Company registered in England number 08059895. VAT number 29475664