

# COVID-19 RELATED CYBER NEWS

Week 9: Saturday 6<sup>th</sup> June to Friday 12<sup>th</sup> June  
Compiled by Barry Gooch

## COVID-19 RELATED ARTICLES

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

### SATURDAY 6<sup>th</sup> June 2020

- **Two Critical Flaws in Zoom Could've Let Attackers Hack Systems via Chat**  
<https://digitpol.com/two-critical-flaws-in-zoom-couldve-let-attackers-hack-systems-via-chat/>
- **New Android Flaw Affecting Over 1 Billion Phones Let Attackers Hijack Apps**  
<https://digitpol.com/new-android-flaw-affecting-over-1-billion-phones-let-attackers-hijack-apps/>
- **Researchers claim lockdown has helped fueled rise in cybercrime in UK**  
<https://www.governmentcomputing.com/security/cybersecurity/lockdown-cybercrime-increase-research>
- **UAE authorities tackle rising cybercrime during COVID-19 pandemic**  
<https://www.euronews.com/2020/06/05/uae-authorities-tackle-rising-cybercrime-during-covid-19-pandemic>
- **Coronavirus Breaks The IT Security Plans**  
<https://www.teceze.com/coronavirus-breaks-the-it-security-plans/>
- **How to dodge cybercriminals & hackers during the COVID-19 pandemic?**  
<https://www.euronews.com/2020/06/05/how-to-dodge-cybercriminals-hackers-during-the-covid-19-pandemic>
- **Furlough fraud: New warning issued as system cheats increase**  
<https://www.express.co.uk/finance/personalfinance/1291451/furlough-fraud-HMRC-job-retention-scheme-UK-CJRS-Rishi-Sunak>
- **Fraud losses from coronavirus scams hit £5m mark**  
<https://www.professionaladviser.com/news/4016158/fraud-losses-coronavirus-scams-hit-gbp-mark>
- **Companies face welter of whistleblowing over fraud and safety**  
<https://www.personneltoday.com/hr/companies-face-welter-of-fraud-and-safety-whistleblowing/>
- **Nearly 80% of Companies Experienced a Cloud Data Breach in Past 18 Months**  
<https://www.securitymagazine.com/articles/92533-nearly-80-of-companies-experienced-a-cloud-data-breach-in-past-18-months>
- **How cybersecurity saves business time and money**  
<https://www.ddls.com.au/blog/how-cybersecurity-saves-business-time-and-money-2/>
- **Be wise to scratchie scams and pyramid schemes**  
<https://www.portstephensexaminer.com.au/story/6742238/scamwatch-if-it-seems-too-good-to-be-true-it-probably-is/>
- **CPA discloses data breach affecting 329K individuals**  
<https://iapp.org/news/a/cpa-discloses-data-breach-affecting-329k-individuals/>

- **Turkey cracks down as cybercrime rises amid pandemic**  
<https://www.aljazeera.com/news/2020/06/turkey-cracks-cybercrime-rises-pandemic-200605110304559.html>
- **How Malaysia is fighting organised cyber crime**  
<https://govinsider.asia/security/haji-amirudin-abdul-wahab-cybersecurity-malaysia-fighting-organised-cyber-crime/>
- **Cybersecurity in the times of coronavirus: Here's how to stay safe**  
<https://indianexpress.com/article/technology/techook/cybersecurity-in-the-times-of-coronavirus-heres-how-to-stay-safe-6320128/>
- **The Cyber Threat Facing Pakistan**  
<https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/>
- **Karnataka Bank reports ₹285-cr. fraud**  
<https://www.thehindu.com/business/karnataka-bank-reports-285-cr-fraud/article31768932.ece>
- **As Iran redeploys amid COVID-19, Russia is filling the vacuum in eastern Syria**  
<https://www.mei.edu/publications/iran-redeploys-amid-covid-19-russia-filling-vacuum-eastern-syria>
- **Coronavirus: RCMP warn Canadians about CERB fraudsters and scams**  
<https://globalnews.ca/news/7035497/coronavirus-rcmp-cerb-fraudsters-scams/>
- **Despite Its Low Cost, Most Consumers Don't Buy Cyber Risk Insurance**  
<https://aleragroup.com/insights/despite-its-low-cost-most-consumers-dont-buy-cyber-risk-insurance-060520/>
- **Fake ransomware decryptor double-encrypts desperate victims' files**  
<https://www.bleepingcomputer.com/news/security/fake-ransomware-decryptor-double-encrypts-desperate-victims-files/>
- **Kind of goes without saying, but fix your admin passwords or risk getting borged by this brute-forcing botnet**  
[https://www.theregister.com/2020/06/05/stealthworker\\_akamai\\_botnet/?&web\\_view=true](https://www.theregister.com/2020/06/05/stealthworker_akamai_botnet/?&web_view=true)
- **Critical Vulnerability Could Have Allowed Hackers to Disrupt Traffic Lights**  
[https://www.securityweek.com/critical-vulnerability-could-have-allowed-hackers-disrupt-traffic-lights/?&web\\_view=true](https://www.securityweek.com/critical-vulnerability-could-have-allowed-hackers-disrupt-traffic-lights/?&web_view=true)

## **SUNDAY 7<sup>th</sup> June 2020**

- **Hackers who hit grid taunt Elexon with dark web files**  
<https://www.telegraph.co.uk/business/2020/06/07/hackers-hit-grid-taunt-elexon-dark-web-files/>
- **Shares in cyber security group soar as digital attacks hit Japan**  
<https://www.ft.com/content/e7fe2bfa-0513-4f15-b34c-e47a08f277b6>
- **Know your limits – LIBOR fraud claim time barred**  
<https://collyerbristow.com/shorter-reads/know-your-limits-libor-fraud-claim-time-barred/>
- **ST Engineering Aerospace's US subsidiary suffers massive data breach**  
<https://www.straitstimes.com/singapore/st-engineering-aerospace-us-subsidiary-suffers-massive-data-breach>
- **Wilful blindness no more: The macro and micro impact of cybersecurity breaches and the imperative for all entities to act now**  
<https://www.nortonrosefulbright.com/en/knowledge/publications/f78aa3b0/wilful-blindness-no-more-the-macro-and-micro-impact-of-cybersecurity-breaches-and-the-imperative>
- **MHA studies tools to monitor darknet**  
<https://www.hindustantimes.com/india-news/mha-studies-tools-to-monitor-darknet/story-yIWPaSJi3fwOwQUvxrzTvJ.html>
- **CBI arrests man in bank fraud case nearly 30 years after family claimed he's dead**  
<https://www.indiatoday.in/india/story/cbi-arrests-man-bank-fraud-case-30-years-after-family-claimed-dea-1686256-2020-06-06>
- **Jump in cyber attacks during Covid-19 confinement – Switzerland**  
<https://www.swissinfo.ch/ger/alle-news-in-kuerze/leck-in-russischem-kraftwerk---500-spezialisten-kaempfen-gegen-folgen/45812394>
- **How to Fight Rise in Cyber Criminals**  
<https://www.insurancethoughtleadership.com/how-to-fight-rise-in-cyber-criminals/>
- **New details on possible data breach at DMV**  
<https://abc7news.com/dmv-california-department-motor-vehicles/14652/>
- **Brazil's Covid Data Blackout is a Tragedy, ex-Health Chief Says**  
<https://www.bloomberg.com/news/articles/2020-06-07/brazil-s-covid-data-blackout-is-a-tragedy-ex-health-chief-says>
- **New Hasty Attempt to Tackle Fake News in Brazil Heavily Strikes Privacy and Free Expression**  
[https://www.eff.org/deeplinks/2020/06/new-hasty-attempt-tackle-fake-news-brazil-heavily-strikes-privacy-and-free?&web\\_view=true](https://www.eff.org/deeplinks/2020/06/new-hasty-attempt-tackle-fake-news-brazil-heavily-strikes-privacy-and-free?&web_view=true)
- **Final Version of NIST SP 1800-23 Guides Identification of Threats to OT Assets**  
[https://www.tripwire.com/state-of-security/regulatory-compliance/final-version-nist-sp-1800-23-guides-identification-threats-assets/?web\\_view=true](https://www.tripwire.com/state-of-security/regulatory-compliance/final-version-nist-sp-1800-23-guides-identification-threats-assets/?web_view=true)

## **MONDAY 8<sup>th</sup> June 2020**

- **Cybercrime is Winning – What Are You Going to Do About It?**  
<https://www.infosecurity-magazine.com/blogs/cybercrime-is-winning/>

- **Protecting the public sector from cybercrime**  
<http://www.publicsectorexecutive.com/The-ravens-daily-blog/protecting-the-public-sector-from-cybercrime-#>
- **How understanding the changing landscape of cybercrime can give you better security**  
<https://www.scmagazineuk.com/understanding-changing-landscape-cybercrime-give-better-security/article/1684099>
- **Regional Cybercrime Centre Announces Trusted Partners**  
<https://bdaily.co.uk/articles/2020/06/08/regional-cybercrime-centre-announces-trusted-partners>
- **Protect yourself from cybercrime while working remotely**  
<https://www.fortpittcapital.com/protect-yourself-from-cybercrime/?cn-reloaded=1>
- **CSN launching first cybercrime victim support hotline in MS**  
<https://www.wlox.com/2020/06/08/csn-launching-first-cybercrime-victim-support-hotline-ms/>
- **Greater cyber security measures needed for COVID-19 crisis**  
<https://seanews.co.uk/security/cyber-security/greater-cyber-security-measures-needed-for-covid-19-crisis/>
- **COVID-19 brings new cyber-security threats to universities**  
<https://www.universityworldnews.com/post.php?story=20200607084916387>
- **Covid-19 leaves maritime sector vulnerable to cyber attacks**  
<https://www.nautilusint.org/en/news-insight/news/covid-19-leaves-maritime-sector-vulnerable-to-cyber-attacks/>
- **Cyber Threats Are Surging As Employees Work From Home Due To The COVID-19 Pandemic, Prompting Cybersecurity Insurers To Reassess Companies' Security Measures—And Potentially Raise Premiums.**  
<https://www.mimecast.com/blog/2020/06/the-impact-of-covid-19-on-cyber-security-insurance/>
- **Honda could be victim of ransomware cyber attack**  
<https://www.telegraph.co.uk/business/2020/06/08/honda-could-victim-ransomware-cyber-attack/>
- **Japanese car giant Honda probes suspected cyber attack**  
<https://news.sky.com/story/japanese-car-giant-honda-probes-suspected-cyber-attack-12002837>
- **When It Comes To Cybersecurity, Covid-19 Tells Us We Do Not Deserve Nice Things**  
<https://www.forbes.com/sites/moorinsights/2020/06/08/when-it-comes-to-cybersecurity-covid-19-tells-us-we-do-not-deserve-nice-things/#38a3fdf27073>
- **Regulator repeats anti-scam warning as £5m lost to fraud**  
<https://www.ftadviser.com/pensions/2020/06/08/regulator-repeats-anti-scam-warning-as-5m-lost-to-fraud/>
- **“SFERS” Suffers Data Breach**  
<https://www.cisomag.com/sfers-suffers-data-breach/>
- **Philippines probes proliferation of fake Facebook accounts after anti-terror law protest**  
<https://in.reuters.com/article/us-philippines-facebook/philippines-probes-proliferation-of-fake-facebook-accounts-after-anti-terror-law-protest-idINKBN23F0K5>
- **The debate over internet governance and cyber crimes: West vs the rest?**  
<https://cis-india.org/internet-governance/blog/the-debate-over-internet-governance-and-cyber-crimes-west-vs-the-rest>
- **Cybersecurity in Nepal: Essential Steps**  
<https://www.bankinfosecurity.asia/cybersecurity-in-nepal-essential-steps-a-14396>
- **Cybersecurity: Beware! Coronavirus-themed attacks on the rise**  
<https://www.financialexpress.com/industry/technology/cybersecurity-beware-coronavirus-themed-attacks-on-the-rise/>
- **PNB Fraud case: PMLA court orders seizure of Nirav Modi's assets worth Rs 1400 crore**  
<https://zeenews.india.com/companies/pnb-fraud-case-pmla-court-orders-seizure-of-nirav-modis-assets-worth-rs-1400-crore-2288839.html>
- **Furlough fraud figures are likely to be the tip of the iceberg – Kennedyslaw**  
<https://www.companynewshq.com/company-news/legal-company-news/furlough-fraud-figures-are-likely-to-be-the-tip-of-the-iceberg-kennedyslaw/>
- **ZEE5 Refutes Report of Data Breach After Hackers Threaten to Leak Customers' Info Online**  
<https://www.news18.com/news/tech/zee5-refutes-report-of-data-breach-after-hackers-threaten-to-leak-customers-info-online-2658599.html>
- **APAC employees not fully secure to work from home**  
<https://www.zdnet.com/article/apac-employees-not-fully-secure-to-work-from-home/>
- **'Drift' to remote working creating future liability and risks**  
<https://www.commercialriskonline.com/drift-to-remote-working-creating-future-liability-and-risks/>
- **AfDB debars firm for 21 months over fraud, corrupt practices**  
<https://nairametrics.com/2020/06/08/afdb-debars-firm-for-21-months-over-fraud-corrupt-practices/>
- **The return of geopolitics will cause global banks considerable headaches**  
<https://www.globalriskregulator.com/Subjects/Reporting-and-Governance/The-return-of-geopolitics-will-cause-global-banks-considerable-headaches>
- **COVID-19 will accelerate cyber insurance uptake as most SMEs have been left vulnerable**  
<https://www.verdict.co.uk/life-insurance-international/comment/covid-19-cyber-insurance-sme/>
- **Risk Professionals Reassess Top Risks During Post-COVID Era**  
<https://www.insurancejournal.com/news/international/2020/06/08/571358.htm>

- **With airline industry brought low, fraud still flying high**  
<https://www.travelweekly.com/Travel-News/Airline-News/With-airline-industry-brought-low-fraud-is-flying-high>
- **Lookers warns over shares suspension after potential fraud found on books**  
<https://www.expressandstar.com/news/motors/2020/06/08/lookers-warns-over-shares-suspension-after-potential-fraud-found-on-books/>
- **New Avaddon Ransomware launches in massive smiley spam campaign**  
<https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/>
- **US energy providers hit with new malware in targeted attacks**  
<https://www.bleepingcomputer.com/news/security/us-energy-providers-hit-with-new-malware-in-targeted-attacks/>
- **Hackers are attacking the German PPE supply chain**  
<https://www.bleepingcomputer.com/news/security/hackers-are-attacking-the-german-ppe-supply-chain/>
- **CallStranger UPnP bug allows data theft, DDoS attacks, LAN scans**  
<https://www.bleepingcomputer.com/news/security/callstranger-upnp-bug-allows-data-theft-ddos-attacks-lan-scans/>
- **Maze Ransomware adds Ragnar Locker to its extortion cartel**  
<https://www.bleepingcomputer.com/news/security/maze-ransomware-adds-ragnar-locker-to-its-extortion-cartel/>
- **Canadian firms lag global peers about cybersecurity risks, says EY survey**  
<https://www.bnnbloomberg.ca/canadian-firms-lag-global-peers-about-cybersecurity-risks-says-ey-survey-1.1447359>
- **South Asia, Middle Eastern regional rivalries play out in cyberspace. Online voting insecurity. PPE supply chain attacks.**  
<https://thecyberwire.com/newsletters/daily-briefing/9/110>
- **Algorithmic Warfare: Undetected Devices May Pose CMMC Issues**  
<https://www.nationaldefensemagazine.org/articles/2020/6/8/undetected-devices-may-pose-cmmc-issues>
- **Multilingual Malware Attacks Against Industrial Sector Suppliers**  
<https://cyware.com/news/multilingual-malware-attacks-against-industrial-sector-suppliers-51de36b5>
- **Capturing the Cyber Threats on Home Base Amidst COVID-19**  
<https://cyware.com/news/capturing-the-cyber-threats-on-home-base-amidst-covid-19-99299e76>
- **Not the Resume You are Looking For**  
<https://cyware.com/news/not-the-resume-you-are-looking-for-c88b3bf1>
- **Owners of DDoS-for-Hire Service vDOS Get 6 Months Community Service**  
[https://krebsonsecurity.com/2020/06/owners-of-ddos-for-hire-service-vdos-get-6-months-community-service/?&web\\_view=true](https://krebsonsecurity.com/2020/06/owners-of-ddos-for-hire-service-vdos-get-6-months-community-service/?&web_view=true)
- **80% hacking attacks linked to bad password habits: Report**  
[https://ciso.economictimes.indiatimes.com/news/80-hacking-attacks-linked-to-bad-password-habits-report/76256068?&web\\_view=true](https://ciso.economictimes.indiatimes.com/news/80-hacking-attacks-linked-to-bad-password-habits-report/76256068?&web_view=true)
- **States scramble to deal with potential spikes in unemployment fraud, prompting Democrats to demand answers**  
[https://www.washingtonpost.com/business/2020/06/08/unemployment-fraud-congress/?&web\\_view=true](https://www.washingtonpost.com/business/2020/06/08/unemployment-fraud-congress/?&web_view=true)
- **IBM releases toolkits for encrypting data while in use**  
[https://www.itpro.co.uk/security/encryption/355961/ibm-releases-toolkits-for-encrypting-data-while-in-use?&web\\_view=true](https://www.itpro.co.uk/security/encryption/355961/ibm-releases-toolkits-for-encrypting-data-while-in-use?&web_view=true)
- **Explained: Everything you need to know about hacktivist group Anonymous**  
[https://indianexpress.com/article/explained/hacktivist-group-anonymous-george-floyd-protests-6446993/?&web\\_view=true](https://indianexpress.com/article/explained/hacktivist-group-anonymous-george-floyd-protests-6446993/?&web_view=true)
- **Fraudulent face mask sites, fake charities: 2020 is 'the perfect storm' for online scams**  
[https://www.yahoo.com/lifestyle/online-scams-covid-protests-software-152737452.html?&web\\_view=true](https://www.yahoo.com/lifestyle/online-scams-covid-protests-software-152737452.html?&web_view=true)
- **German Task Force for COVID-19 Medical Equipment Targeted in Ongoing Phishing Campaign**  
[https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/?&web\\_view=true](https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/?&web_view=true)
- **Is a 'Cyber Pandemic' Coming?**  
[https://www.govtech.com/blogs/lohmann-on-cybersecurity/is-a-cyber-pandemic-coming.html?&web\\_view=true](https://www.govtech.com/blogs/lohmann-on-cybersecurity/is-a-cyber-pandemic-coming.html?&web_view=true)
- **Third of people 'hold chief executive personally responsible for cyber attacks'**  
[https://uk.finance.yahoo.com/news/third-people-hold-chief-executive-230100786.html?&web\\_view=true](https://uk.finance.yahoo.com/news/third-people-hold-chief-executive-230100786.html?&web_view=true)
- **Korean credit card data leaked overseas, group reports**  
[https://en.yna.co.kr/view/AEN20200608011200325?&web\\_view=true](https://en.yna.co.kr/view/AEN20200608011200325?&web_view=true)
- **Canada's Fitness Depot Alerts Customers to Data Breach**  
<https://www.darkreading.com/attacks-breaches/canadas-fitness-depot-alerts-customers-to-data-breach/d/d-id/1338025>
- **Malware found in popular barcode apps produces ads that instantly vanish**  
<https://www.scmagazine.com/home/security-news/malware/malware-found-in-popular-barcode-apps-produces-ads-that-instantly-vanish/>

## **TUESDAY 9<sup>th</sup> June 2020**

- **Military members are disproportionately affected by cybercrime: Here's why and how to avoid it**  
<https://www.militarytimes.com/2020/06/10/military-members-are-disproportionately-affected-by-cybercrime-heres-why-and-how-to-avoid-it/>
- **Cybercrime against retail brands is up 41% during pandemic**  
<https://www.techrepublic.com/article/cybercrime-against-retail-brands-is-up-41-during-pandemic/>
- **Cybercrime: How to protect your investments from hackers**  
<https://www.portfolio-institutional.co.uk/features/cybercrime-how-to-protect-your-investments-from-hackers/>
- **Four ways FIs can stay ahead of cybercrime during and beyond COVID-19**  
<https://www.sc.com/en/feature/four-ways-fis-can-stay-ahead-of-cybercrime-during-and-beyond-covid-19/>
- **Cyber security post-COVID-19**  
<https://www.techuk.org/insights/news/item/17869-cyber-security-post-covid-19>
- **Working from home? Stay alert to the risk of cyber-attacks**  
<https://boardagenda.com/2020/06/09/working-from-home-stay-alert-to-the-risk-of-cyber-attacks/>
- **Honda's global factories brought to a standstill by cyber attack**  
<https://www.telegraph.co.uk/technology/2020/06/09/hondas-global-factories-brought-standstill-cyber-attack/>
- **Remote Workers Warned Of Data Security Vulnerability During COVID-19**  
<https://www.onrec.com/news/news-archive/remote-workers-warned-of-data-security-vulnerability-during-covid-19>
- **Securing the 'new normal' – survey shows organizations' security priorities as they emerge from Covid-19 lockdown**  
<https://www.globenewswire.com/news-release/2020/06/09/2045445/0/en/Securing-the-new-normal-survey-shows-organizations-security-priorities-as-they-emerge-from-Covid-19-lockdown.html>
- **Local councils urged to tackle procurement fraud**  
<https://www.accountancydaily.co/local-councils-urged-tackle-procurement-fraud>
- **Suffolk financial adviser jailed for £300k fraud**  
<https://www.bbc.co.uk/news/uk-england-suffolk-52985524>
- **Why do you need fraud prevention?**  
<https://www.adjust.com/blog/why-you-need-fraud-prevention/>
- **Babylon Health admits GP app suffered a data breach**  
<https://www.bbc.co.uk/news/technology-52986629>
- **Keepnet Labs confirms contractor exposed 'data breach database' of 5 billion records**  
<https://www.verdict.co.uk/keepnet-labs-data-breach/>
- **Data breach leads to the theft of \$10M from a Norwegian investment fund**  
<https://www.pandasecurity.com/mediacenter/business/data-breach-theft-norfund/>
- **Report: Average data breach costs public companies \$116M**  
<https://www.complianceweek.com/cyber-security/report-average-data-breach-costs-public-companies-116m/29037.article>
- **COVID has made Australia 'less safe': ASIO boss**  
<https://www.smh.com.au/politics/federal/covid-has-made-australia-less-safe-asio-boss-20200608-p550hv.html>
- **COVID-19: Malicious emails are driving a cyber-crime pandemic**  
<https://www.hcamag.com/au/specialisation/hr-technology/covid-19-malicious-emails-are-driving-a-cyber-crime-pandemic/224664>
- **COVID-19 – What are the phishing scams to watch out for**  
<https://www.teiss.co.uk/covid-19-what-are-the-phishing-scams-to-watch-out-for/>
- **THE INDUSTRY WIDE FRAUD MITIGATION FRAMEWORK**  
<https://www.nab.com.au/business/payments-and-merchants/merchant-support-centre/card-not-present-fraud>
- **Vast Majority of Australian Companies Believe Their Cybersecurity Is Failing**  
<https://securityboulevard.com/2020/06/vast-majority-of-australian-companies-believe-their-cybersecurity-is-failing/>
- **Cyber-Crime During The Covid-19 Pandemic**  
<http://www.legalserviceindia.com/legal/article-2687-cyber-crime-during-the-covid-19-pandemic.html>
- **The obscure Indian hackers for hire who spied on global elites**  
<https://www.aljazeera.com/ajimpact/obscure-indian-hackers-hire-spied-global-elites-200609132902369.html>
- **South Africa's Life Healthcare hit by cyber attack**  
<https://in.reuters.com/article/us-life-healthcare-cyber/south-africas-life-healthcare-hit-by-cyber-attack-idINKBN23G0MY>
- **Natura & Co says 'cyber incident' partially hit Avon operations; shares fall**  
<https://in.reuters.com/article/us-natura-cyber-incident/natura-co-says-cyber-incident-partially-hit-avon-operations-shares-fall-idINKBN23G24J>
- **Vietnamese operators fined for SIM registration fraud**  
<https://www.developingtelecoms.com/telecom-business/telecom-regulation/9631-vietnamese-operators-fined-for-sim-registration-fraud.html>
- **BEML's internal data, staff email IDs hacked, leaked on dark web**  
<https://www.thehindu.com/news/cities/mumbai/bemls-internal-data-staff-email-ids-hacked-leaked-on-dark-web/article31790702.ece>

- **Phishing Attacks Traced to Indian Commercial Espionage Firm**  
<https://www.bankinfosecurity.com/phishing-attacks-traced-to-indian-commercial-espionage-firm-a-14406>
- **Iran-Israel cyberattacks threaten unofficial rules of engagement**  
<https://www.pri.org/stories/2020-06-09/iran-israel-cyberattacks-threaten-unofficial-rules-engagement>
- **COVID-19 Is Breeding More Cyberattacks: Here's How to Contain Them**  
<https://www.hysolate.com/blog/containing-cyber-attacks/>
- **Ransomware attacks soar 25% during COVID-19 crisis**  
<https://www.theactuary.com/2020/06/09/ransomware-attacks-soar-25-during-covid-19-crisis>
- **Valak malware gets new plugin to steal Outlook login credentials**  
<https://www.bleepingcomputer.com/news/security/valak-malware-gets-new-plugin-to-steal-outlook-login-credentials/>
- **Adobe fixes critical remote code execution bug in Flash Player**  
<https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-remote-code-execution-bug-in-flash-player/>
- **New SGAXe attack steals protected data from Intel SGX enclaves**  
<https://www.bleepingcomputer.com/news/security/new-sgaxe-attack-steals-protected-data-from-intel-sgx-enclaves/>
- **Intel patched 22 vulnerabilities in the June 2020 Platform Update**  
<https://www.bleepingcomputer.com/news/security/intel-patched-22-vulnerabilities-in-the-june-2020-platform-update/>
- **Windows Group Policy flaw lets attackers gain admin privileges**  
<https://www.bleepingcomputer.com/news/security/windows-group-policy-flaw-lets-attackers-gain-admin-privileges/>
- **Fake SpaceX YouTube channels scam viewers out of \$150K in bitcoin**  
<https://www.bleepingcomputer.com/news/security/fake-spacex-youtube-channels-scam-viewers-out-of-150k-in-bitcoin/>
- **ANALYSIS: Hitting the Pause Button on Contact Tracing**  
<https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-hitting-the-pause-button-on-contact-tracing>
- **Wake Up Call: Surge in Covid Litigation Work in View, Survey Says**  
<https://news.bloomberglaw.com/business-and-practice/wake-up-call-surge-in-covid-litigation-work-in-view-survey-says>
- **Understanding Payload-Less Email Attacks**  
<https://cyware.com/news/understanding-payload-less-email-attacks-65389771>
- **Tycoon Ransomware Aims at Software and Education Sector**  
<https://cyware.com/news/tycoon-ransomware-aims-at-software-and-education-sector-ea55753e>
- **Do Not Let Fleeceware Fool You**  
<https://cyware.com/news/do-not-let-fleeceware-fool-you-5954808c>
- **Zorab Ransomware Doubles the Pain of 'STOP Djvu' Ransomware Victims**  
<https://cyware.com/news/zorab-ransomware-doubles-the-pain-of-stop-djvu-ransomware-victims-35e0ab29>
- **SMBGhost - Ghosts of the SMB Bugs Still Haunting Security Researchers**  
<https://cyware.com/news/smbghost-ghosts-of-the-smb-bugs-still-haunting-security-researchers-e087b99f>
- **Maze Ransomware Does It Again, This Time Targets US Aerospace Services Provider**  
<https://cyware.com/news/maze-ransomware-does-it-again-this-time-targets-us-aerospace-services-provider-07a1dacd>
- **Because things aren't bad enough already: COVID-19 is going to mess up election security assumptions too**  
[https://www.theregister.co.uk/2020/06/08/lockdown\\_election\\_hacking/?&web\\_view=true](https://www.theregister.co.uk/2020/06/08/lockdown_election_hacking/?&web_view=true)
- **A Vulnerability in IBM WebSphere Application Server Could Allow for Remote Code Execution**  
[https://www.cisecurity.org/advisory/a-vulnerability-in-ibm-websphere-application-server-could-allow-for-remote-code-execution\\_2020-078/?&web\\_view=true](https://www.cisecurity.org/advisory/a-vulnerability-in-ibm-websphere-application-server-could-allow-for-remote-code-execution_2020-078/?&web_view=true)
- **New Avaddon Ransomware launches in massive smiley spam campaign**  
[https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/?&web\\_view=true](https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/?&web_view=true)
- **2019 was a record year for OSS vulnerabilities**  
[https://www.helpnetsecurity.com/2020/06/09/oss-vulnerabilities/?&web\\_view=true](https://www.helpnetsecurity.com/2020/06/09/oss-vulnerabilities/?&web_view=true)
- **Administration's cyber defense plan stresses 'Made in USA'**  
[https://gcn.com/articles/2020/06/08/domestic-bulk-power-components-cybersecurity.aspx?&web\\_view=true](https://gcn.com/articles/2020/06/08/domestic-bulk-power-components-cybersecurity.aspx?&web_view=true)
- **NASA Hit By 366% Rise In Cybersecurity Incidents After Budget Cuts**  
[https://www.forbes.com/sites/simonchandler/2020/06/08/nasa-hit-by-366-rise-in-cybersecurity-incidents-after-budget-cuts/?&web\\_view=true](https://www.forbes.com/sites/simonchandler/2020/06/08/nasa-hit-by-366-rise-in-cybersecurity-incidents-after-budget-cuts/?&web_view=true)
- **BRIEF: Minnesota School District Addresses Cybersecurity Breach**  
[https://www.govtech.com/security/BRIEF-Minnesota-School-District-Addresses-Cybersecurity-Breach.html?&web\\_view=true](https://www.govtech.com/security/BRIEF-Minnesota-School-District-Addresses-Cybersecurity-Breach.html?&web_view=true)
- **Are Academic Healthcare Systems Top COVID-19 Attack Targets?**  
[https://www.inforisktoday.com/are-academic-healthcare-systems-top-covid-19-attack-targets-a-14403?&web\\_view=true](https://www.inforisktoday.com/are-academic-healthcare-systems-top-covid-19-attack-targets-a-14403?&web_view=true)
- **US energy providers hit with new malware in targeted attacks**  
[https://www.bleepingcomputer.com/news/security/us-energy-providers-hit-with-new-malware-in-targeted-attacks/?&web\\_view=true](https://www.bleepingcomputer.com/news/security/us-energy-providers-hit-with-new-malware-in-targeted-attacks/?&web_view=true)
- **Study finds vulnerabilities in online voting tool used by several states**  
[https://thehill.com/policy/cybersecurity/501723-study-finds-security-vulnerabilities-in-online-voting-tool-used-in?&web\\_view=true](https://thehill.com/policy/cybersecurity/501723-study-finds-security-vulnerabilities-in-online-voting-tool-used-in?&web_view=true)

- **Ransomware Strikes Third US College in a Week**  
[https://www.infosecurity-magazine.com/news/ransomware-strikes-third-us/?&web\\_view=true](https://www.infosecurity-magazine.com/news/ransomware-strikes-third-us/?&web_view=true)
- **Microsoft Predicts Escalation of Zero Trust in Lockdown Environments**  
[https://www.infosecurity-magazine.com/news/microsoft-zero-trust-lockdown/?&web\\_view=true](https://www.infosecurity-magazine.com/news/microsoft-zero-trust-lockdown/?&web_view=true)
- **Security Drift – The Silent Killer**  
[https://thehackernews.com/2020/06/security-drift-silent-killer.html?&web\\_view=true](https://thehackernews.com/2020/06/security-drift-silent-killer.html?&web_view=true)
- **Paid hackers targeted thousands of people and hundreds of institutions worldwide, report says**  
[https://www.latimes.com/world-nation/story/2020-06-09/paid-hackers-dark-basin-targeted-thousands-people-hundreds-institutions?&web\\_view=true](https://www.latimes.com/world-nation/story/2020-06-09/paid-hackers-dark-basin-targeted-thousands-people-hundreds-institutions?&web_view=true)
- **Beware—20 Million Android Users Have Now Installed These ‘Malicious’ Photo Apps**  
[https://www.forbes.com/sites/zakdoffman/2020/06/09/beware-20-million-android-users-must-remove-these-malicious-camera-apps-now/?&web\\_view=true](https://www.forbes.com/sites/zakdoffman/2020/06/09/beware-20-million-android-users-must-remove-these-malicious-camera-apps-now/?&web_view=true)
- **Op-ed: The 'silver lining' of the pandemic is the way it is catalyzing changes in cybersecurity**  
[https://www.cnbc.com/2020/06/09/silver-lining-of-pandemic-is-how-it-may-spark-shift-in-cybersecurity.html?&web\\_view=true](https://www.cnbc.com/2020/06/09/silver-lining-of-pandemic-is-how-it-may-spark-shift-in-cybersecurity.html?&web_view=true)
- **Cybercrime against retail brands is up 41% during pandemic**  
[https://www.techrepublic.com/article/cybercrime-against-retail-brands-is-up-41-during-pandemic/?&web\\_view=true](https://www.techrepublic.com/article/cybercrime-against-retail-brands-is-up-41-during-pandemic/?&web_view=true)
- **Getting Ahead of Cybersecurity Disasters**  
[https://www.infosecurity-magazine.com/opinions/ahead-cyber-disasters/?&web\\_view=true](https://www.infosecurity-magazine.com/opinions/ahead-cyber-disasters/?&web_view=true)
- **Search traffic reveals 'mad scramble' for cybersecurity at pandemic peak**  
[https://www.itproportal.com/news/search-traffic-reveals-mad-scramble-for-cybersecurity-at-pandemic-peak/?&web\\_view=true](https://www.itproportal.com/news/search-traffic-reveals-mad-scramble-for-cybersecurity-at-pandemic-peak/?&web_view=true)
- **Remote working creates a gap in cyber security for companies: Report**  
[https://telecom.economictimes.indiatimes.com/news/remote-working-creates-a-gap-in-cyber-security-for-companies-report/76282876?&web\\_view=true](https://telecom.economictimes.indiatimes.com/news/remote-working-creates-a-gap-in-cyber-security-for-companies-report/76282876?&web_view=true)
- **Report: How hack-for-hire group Dark Basin wreaks havoc**  
<https://www.scmagazine.com/home/security-news/report-how-hack-for-hire-dark-basin-wreaks-havoc/>

### **WEDNESDAY 10<sup>th</sup> June 2020**

- **How cybercrime has changed in the wake of COVID-19**  
<https://www.techradar.com/uk/news/how-cybercrime-has-changed-in-the-wake-of-covid-19>
- **Unsecured Elasticsearch server breached in eight hours flat**  
<https://www.computerweekly.com/news/252484365/Unsecured-ElasticSearch-server-breached-in-eight-hours-flat>
- **Decade-old vulnerability among 129 Patch Tuesday fixes**  
<https://www.computerweekly.com/news/252484442/Decade-old-vulnerability-among-129-Patch-Tuesday-fixes>
- **Nigerian journalist held under cybercrime act for COVID-19 coverage**  
<https://cpi.org/2020/06/nigerian-journalist-held-under-cybercrime-act-for-covid-19-coverage/>
- **A Crisis in a Crisis: Managing Cyber Attacks During COVID-19**  
<https://www.fsmatters.com/Crisis-Management-During-COVID-19>
- **Eurojust supports new major crackdown on fraud with pay TV**  
<http://eurojust.europa.eu/press/PressReleases/Pages/2020/2020-06-10.aspx>
- **Natura's Avon suffers 'cyber incident' weeks after major data breach**  
[https://cosmeticsbusiness.com/news/article\\_page/Naturas\\_Avon\\_suffers\\_cyber\\_incident\\_weeks\\_after\\_major\\_data\\_breach/166378](https://cosmeticsbusiness.com/news/article_page/Naturas_Avon_suffers_cyber_incident_weeks_after_major_data_breach/166378)
- **Lion hit by cyber attack**  
<https://www.drinkstrade.com.au/lion-hit-by-cyber-attack>
- **How cybercrime has changed in the wake of COVID-19**  
<https://www.techradar.com/nz/news/how-cybercrime-has-changed-in-the-wake-of-covid-19>
- **Australia: Stop the spread: Cyber hygiene during COVID-19**  
<https://www.mondaq.com/australia/security/950942/stop-the-spread-cyber-hygiene-during-covid-19>
- **Australia is unprepared for cyber war**  
<https://www.csoonline.com/article/3561752/australia-is-unprepared-for-cyber-war.html>
- **Coronavirus: pandemic has increased cyber vulnerabilities for businesses, governments, as ASIO says Australia is 'less safe'**  
<https://www.canberratimes.com.au/story/6786092/pandemic-has-increased-cyber-security-risks-for-government-and-businesses/#qsc.tab=0>
- **Coronavirus: How to go back to the office safely and securely**  
<https://www.computerweekly.com/feature/Coronavirus-How-to-go-back-to-the-office-safely-and-securely>
- **Companies seek help for post-redundancy data breaches**  
<https://www.rnz.co.nz/news/business/418695/companies-seek-help-for-post-redundancy-data-breaches>
- **India records Cyber Crime cases during Corona Period**  
<https://m.dailyhunt.in/news/india/english/newstrack+journalism+english-epaper-nwstkgeng/india+records+cyber+crime+cases+during+corona+period-newsid-n190384228>

- **Fugitive Indian tycoon Vijay Mallya applies for UK asylum**  
<https://www.theguardian.com/law/2020/jun/10/fugitive-indian-tycoon-vijay-mallya-applies-for-uk-asylum>
- **Selfie apps riddled with fraud, and brands are inadvertently funding them**  
<https://www.campaignasia.com/article/selfie-apps-riddled-with-fraud-and-brands-are-inadvertently-funding-them/461540>
- **Feds investigating hacker ring paid to target corporate critics**  
<https://www.securityinfowatch.com/cybersecurity/news/21141668/feds-investigating-hacker-ring-paid-to-target-corporate-critics>
- **In India, Mandatory COVID App Raises Privacy and Data-Theft Issues**  
<https://digitalprivacy.news/2020/06/10/in-india-mandatory-covid-app-raises-privacy-and-data-theft-issues/>
- **How Australian firms can defend against supply chain attacks**  
<https://www.computerweekly.com/news/252484430/How-Australian-firms-can-defend-against-supply-chain-attacks>
- **Mimecast State of Email Security 2020 report reveals 60% of organisations expect to suffer from an email-borne attack**  
<https://australiancybersecuritymagazine.com.au/mimecast-state-of-email-security-2020-report-reveals-60-of-organisations-expect-to-suffer-from-an-email-borne-attack/>
- **The Ticking Timebomb: Data Breaches from Hardware End-of-Life**  
<https://www.infosecurity-magazine.com/blogs/data-breaches-hardware-endoflife/>
- **South Africa: Insurance, finance and retail most at risk from cyber crime**  
<https://www.meinsurancereview.com/News/View-NewsLetter-Article?id=62102&Type=MiddleEast>
- **Scammers pushing new 'Ponzi' scheme over WhatsApp in South Africa**  
<https://businesstech.co.za/news/finance/406433/scammers-pushing-new-ponzi-scheme-over-whatsapp-in-south-africa/>
- **Staying cyber healthy**  
<https://www.rcmp-grc.gc.ca/en/cyber-safety/staying-cyber-healthy?re>
- **COVID-19 Canadian Immigration Fraud on the Rise**  
<https://canadianvisa.org/blog/news/covid-19-canadian-immigration-fraud-on-the-rise>
- **What to Know About Cyber Security and Patents**  
<https://www.thepatent.news/2020/06/11/what-to-know-about-cyber-security-and-patents/>
- **Essential cybersecurity guidelines to protect your business**  
<https://www.hotelmanagement.com.au/2020/06/10/essential-cybersecurity-guidelines-to-protect-your-business/>
- **Ever-present cyber risk exacerbated by pandemic**  
<https://www.insurancebusinessmag.com/ca/news/cyber/everpresent-cyber-risk-exacerbated-by-pandemic-224811.aspx>
- **Allianz and BAE Systems on insurance fraud during the coronavirus**  
<https://www.insurancebusinessmag.com/uk/news/breaking-news/allianz-and-bae-systems-on-insurance-fraud-during-the-coronavirus-224794.aspx>
- **Trends in hotel and restaurant data breaches**  
<https://www.hotelnewsnow.com/Articles/303070/Trends-in-hotel-and-restaurant-data-breaches>
- **Self-destructing skimmer steals credit cards of Greenworks customers**  
<https://www.bleepingcomputer.com/news/security/self-destructing-skimmer-steals-credit-cards-of-greenworks-customers/>
- **Kingminer patches vulnerable servers to lock out competitors**  
<https://www.bleepingcomputer.com/news/security/kingminer-patches-vulnerable-servers-to-lock-out-competitors/>
- **New Windows 10 SMBv3 flaw can be used for data theft, RCE attacks**  
<https://www.bleepingcomputer.com/news/security/new-windows-10-smbv3-flaw-can-be-used-for-data-theft-rce-attacks/>
- **FBI warns of increased hacking risk if using mobile banking apps**  
<https://www.bleepingcomputer.com/news/security/fbi-warns-of-increased-hacking-risk-if-using-mobile-banking-apps/>
- **Microsoft Office June security updates fix critical RCE bugs**  
<https://www.bleepingcomputer.com/news/security/microsoft-office-june-security-updates-fix-critical-rce-bugs/>
- **Office 365 phishing baits business owners with relief payments**  
<https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-business-owners-with-relief-payments/>
- **Expiring SSL certs expected to break smart TVs, fridges, and IoTs**  
<https://www.bleepingcomputer.com/news/security/expiring-ssl-certs-expected-to-break-smart-tvs-fridges-and-iots/>
- **Fake Black Lives Matter voting campaign spreads Trickbot malware**  
<https://www.bleepingcomputer.com/news/security/fake-black-lives-matter-voting-campaign-spreads-trickbot-malware/>
- **China, Russia Are Spreading Virus Misinformation, EU Says**  
<https://www.bloomberg.com/news/articles/2020-06-10/eu-points-finger-at-china-russia-for-covid-19-disinformation>
- **DHS's cyber wing pledges to invest more in industrial control systems security**  
[https://www.cyberscoop.com/dhs-cisa-industrial-control-system-security-strategy/?web\\_view=true](https://www.cyberscoop.com/dhs-cisa-industrial-control-system-security-strategy/?web_view=true)
- **Researchers Identify Multiple vulnerabilities in Siemens LOGO! PLC**  
[https://blog.talosintelligence.com/2020/06/vuln-spotlight-siemens-logo-june-2020.html?web\\_view=true](https://blog.talosintelligence.com/2020/06/vuln-spotlight-siemens-logo-june-2020.html?web_view=true)
- **Coronavirus cyber hygiene and the IT manager's responsibility**  
[https://gcn.com/articles/2020/06/09/cyber-hygiene-post-covid.aspx?web\\_view=true](https://gcn.com/articles/2020/06/09/cyber-hygiene-post-covid.aspx?web_view=true)
- **Bogus tax refund emails sent to students tell them to watch out for scams**  
[https://uk.finance.yahoo.com/news/bogus-tax-refund-emails-sent-150841202.html?web\\_view=true](https://uk.finance.yahoo.com/news/bogus-tax-refund-emails-sent-150841202.html?web_view=true)



- **FCC failed to monitor Chinese telecoms for almost 20 years: Senate report**  
[https://arstechnica.com/tech-policy/2020/06/fcc-failed-to-monitor-chinese-telecoms-for-almost-20-years-senate-report/?&web\\_view=true](https://arstechnica.com/tech-policy/2020/06/fcc-failed-to-monitor-chinese-telecoms-for-almost-20-years-senate-report/?&web_view=true)
- **GnuTLS patches huge security hole that hung around for two years**  
[https://www.theregister.co.uk/2020/06/10/gnutls\\_patches\\_security\\_hole/?&web\\_view=true](https://www.theregister.co.uk/2020/06/10/gnutls_patches_security_hole/?&web_view=true)
- **Senior official estimates \$30 billion in stimulus funds will be stolen through coronavirus scams**  
[https://thehill.com/policy/cybersecurity/501936-senior-official-estimates-30-billion-in-stimulus-funds-will-be-stolen/?&web\\_view=true](https://thehill.com/policy/cybersecurity/501936-senior-official-estimates-30-billion-in-stimulus-funds-will-be-stolen/?&web_view=true)
- **Cyber Command creates new malware sharing portal with National Guard**  
[https://www.defensenews.com/dod/cybercom/2020/06/09/cyber-command-creates-new-malware-sharing-portal-with-national-guard/?&web\\_view=true](https://www.defensenews.com/dod/cybercom/2020/06/09/cyber-command-creates-new-malware-sharing-portal-with-national-guard/?&web_view=true)
- **Adobe Warns of Critical Flaws in Flash Player, Framemaker**  
[https://threatpost.com/adobe-warns-critical-flaws-flash-player-frames-maker/156417/?&web\\_view=true](https://threatpost.com/adobe-warns-critical-flaws-flash-player-frames-maker/156417/?&web_view=true)
- **Arm CPUs impacted by rare side-channel attack**  
[https://www.zdnet.com/article/arm-cpus-impacted-by-rare-side-channel-attack/?&web\\_view=true](https://www.zdnet.com/article/arm-cpus-impacted-by-rare-side-channel-attack/?&web_view=true)
- **Florence, Ala. Hit By Ransomware 12 Days After Being Alerted by KrebsOnSecurity**  
[https://krebsonsecurity.com/2020/06/florence-ala-hit-by-ransomware-12-days-after-being-alerted-by-krebsonsecurity/?&web\\_view=true](https://krebsonsecurity.com/2020/06/florence-ala-hit-by-ransomware-12-days-after-being-alerted-by-krebsonsecurity/?&web_view=true)
- **Microsoft June 2020 Patch Tuesday fixes 129 vulnerabilities**  
[https://www.zdnet.com/article/microsoft-june-2020-patch-tuesday-fixes-129-vulnerabilities/?&web\\_view=true](https://www.zdnet.com/article/microsoft-june-2020-patch-tuesday-fixes-129-vulnerabilities/?&web_view=true)
- **Plundering of crypto keys from ultrasecure SGX sends Intel scrambling again**  
[https://arstechnica.com/information-technology/2020/06/new-exploits-plunder-crypto-keys-and-more-from-intels-ultrasecure-sgx/?&web\\_view=true](https://arstechnica.com/information-technology/2020/06/new-exploits-plunder-crypto-keys-and-more-from-intels-ultrasecure-sgx/?&web_view=true)
- **F&P Appliances latest to be hit by ransomware attack**  
[https://www.nzherald.co.nz/business/news/article.cfm?c\\_id=3&objectid=12338832&web\\_view=true](https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12338832&web_view=true)
- **A 'new normal' in cyberwar should scare us to action**  
[https://www.japantimes.co.jp/opinion/2020/06/10/commentary/world-commentary/new-normal-cyberwar-scare-us-action/?&web\\_view=true](https://www.japantimes.co.jp/opinion/2020/06/10/commentary/world-commentary/new-normal-cyberwar-scare-us-action/?&web_view=true)
- **Nintendo Confirms Over 300,000 Accounts Compromised After Cyberattack**  
[https://in.mashable.com/tech/14655/nintendo-confirms-over-300000-accounts-compromised-after-cyberattack/?&web\\_view=true](https://in.mashable.com/tech/14655/nintendo-confirms-over-300000-accounts-compromised-after-cyberattack/?&web_view=true)
- **Unsecured honeypot database witnesses 18 attacks per day on average**  
[https://www.comparitech.com/blog/information-security/unsecured-database-honeypot/?&web\\_view=true](https://www.comparitech.com/blog/information-security/unsecured-database-honeypot/?&web_view=true)
- **Ransomware Gang Partnerships: Formation of Cartels**  
<https://cyware.com/news/ransomware-gang-partnerships-formation-of-cartels-2895e8a6>
- **US Companies Lost Over \$1.2 Trillion Due to Data Breaches in 2019**  
<https://cyware.com/news/us-companies-lost-over-12-trillion-due-to-data-breaches-in-2019-0f2e319d>
- **Organizations are creating the perfect storm by not implementing security basics**  
<https://www.helpnetsecurity.com/2020/06/10/implementing-security-basics/>
- **Helping Remote Workers Overcome Remote Attacks**  
<https://threatpost.com/helping-remote-workers-remote-attacks/156467/>

## **THURSDAY 11<sup>th</sup> May 2020**

- **Cyber crime shoots up in lockdown, over 2000 cases reported till April**  
<https://www.newindianexpress.com/states/karnataka/2020/jun/11/cyber-crime-shoots-up-in-lockdown-over-2k-cases-reported-till-april-2155009.html>
- **Fraud is going up – is your business prepared?**  
<https://www.financialdirector.co.uk/2020/06/11/fraud-is-going-up-is-your-business-prepared/>
- **Cybercrime Squad detectives lay nine additional charges over \$3.6 million scam, NSW**  
<https://www.nationaltribune.com.au/cybercrime-squad-detectives-lay-nine-additional-charges-over-36-million-scam-nsw/>
- **New Zealand named amongst most vulnerable countries at risk of cyber attack**  
<https://securitybrief.eu/story/new-zealand-named-amongst-most-vulnerable-countries-at-risk-of-cyber-attack>
- **Coronavirus: Bungled British response leads to rise in security risks**  
<https://www.computerweekly.com/news/252484503/Coronavirus-Bungled-British-response-leads-to-rise-in-security-risks>
- **Police bust Dept of Finance workers for alleged IT contract fraud**  
<https://www.arnnet.com.au/article/680447/police-bust-dept-of-finance-workers-for-alleged-it-contract-fraud/>
- **Businessman Rodney McCall pleads guilty in fake foreign investment fraud case**  
[https://www.nzherald.co.nz/business/news/article.cfm?c\\_id=3&objectid=12339146](https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12339146)
- **'Increase' in 'Wangiri-type' phone call scams prompts warning from telcos**  
<https://www.newshub.co.nz/home/new-zealand/2020/06/increase-in-wangiri-type-phone-call-scams-prompts-warning-from-telcos.html>
- **Talks with TLS: Thoughts from an International Cybersecurity Expert**  
<https://www.jdsupra.com/legalnews/talks-with-tls-thoughts-from-an-56807>

- **'A breach of privacy': Government issues reminder to hospitality sector over contact tracing details**  
<https://www.newshub.co.nz/home/lifestyle/2020/06/a-breach-of-privacy-government-issues-reminder-to-hospitality-sector-over-contact-tracing-details.html>
- **Indian organisations faced 14.6 crore malware attacks in 2019**  
<https://government.economictimes.indiatimes.com/news/digital-india/indian-organisations-faced-14-6-crore-malware-attacks-in-2019/73200478>
- **Facebook is suing an Indian company for domain name fraud**  
[http://timesofindia.indiatimes.com/articleshow/76313830.cms?utm\\_source=contentofinterest&utm\\_medium=text&utm\\_campaign=cppst](http://timesofindia.indiatimes.com/articleshow/76313830.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst)
- **Federal Bank of India Combats Card and Merchant Fraud with ACI Worldwide's UP Payments Risk Management Solution**  
<https://www.businesswire.com/news/home/20200611005329/en/Federal-Bank-India-Combats-Card-Merchant-Fraud>
- **Living below the cyber poverty line: strategic challenges for Africa**  
<https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/>
- **The 'new normal' as cyber-spies navigate pandemic**  
<https://www.bbc.co.uk/news/technology-52992677>
- **Mercy Corps Says More Than \$600,000 Lost in Congo Aid Scam**  
<https://www.nytimes.com/reuters/2020/06/11/world/africa/11reuters-congo-aid.html>
- **Latin America: Compliance During COVID-19**  
<https://www.latinvex.com/app/article.aspx?id=4691>
- **Reading Crown Court: Hungerford man avoids jail for computer hacking**  
<https://www.newburytoday.co.uk/news/news/30909/reading-crown-court-hungerford-man-avoids-jail-for-computer-hacking.html>
- **New cyber threat takes top spot as number one cause of loss**  
<https://www.insurancebusinessmag.com/us/news/cyber/new-cyber-threat-takes-top-spot-as-number-one-cause-of-loss-224920.aspx>
- **Simple steps towards cyber-crime prevention for the agricultural sector**  
<https://www.marshcommercial.co.uk/articles/simple-steps-towards-cybercrime-prevention/>
- **Why companies need to be extra vigilant about IT security during COVID-19**  
<https://www.keystonelaw.com/keynotes/why-companies-need-to-be-extra-vigilant-about-it-security-during-covid-19>
- **Are airports and airlines prepared for cyber threats post COVID-19?**  
<https://www.cybersecurity-insiders.com/are-airports-and-airlines-prepared-for-cyber-threats-post-covid-19/+&cd=12&hl=en&ct=clnk&gl=uk&client=opera>
- **Is jailed Anbang founder involved in US hotel fraud?**  
[https://www.koreatimes.co.kr/www/biz/2020/06/602\\_291053.html](https://www.koreatimes.co.kr/www/biz/2020/06/602_291053.html)
- **Gamaredon hackers use Outlook macros to spread malware to contacts**  
<https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/>
- **Turn the Table on Phishers and Scammers to Protect Your Brand**  
<https://www.bleepingcomputer.com/news/security/turn-the-table-on-phishers-and-scammers-to-protect-your-brand/>
- **Power company Enel Group suffers Snake Ransomware attack**  
<https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/>
- **City of Knoxville shuts down network after ransomware attack**  
<https://www.bleepingcomputer.com/news/security/city-of-knoxville-shuts-down-network-after-ransomware-attack/>
- **Fortune 500 insurance firm Genworth discloses data breach**  
[www.bleepingcomputer.com/news/security/fortune-500-insurance-firm-genworth-discloses-data-breach/](http://www.bleepingcomputer.com/news/security/fortune-500-insurance-firm-genworth-discloses-data-breach/)
- **Live event solutions leader TAIT discloses data breach**  
<https://www.bleepingcomputer.com/news/security/live-event-solutions-leader-tait-discloses-data-breach/>
- **George Floyd: Microsoft bars facial recognition sales to police**  
<https://www.bbc.co.uk/news/business-53015468>
- **Rate of Ransomware Attacks in Healthcare Slows in H1 2020**  
[https://www.darkreading.com/attacks-breaches/rate-of-ransomware-attacks-in-healthcare-slows-in-h1-2020/d-d-id/1338051?&web\\_view=true](https://www.darkreading.com/attacks-breaches/rate-of-ransomware-attacks-in-healthcare-slows-in-h1-2020/d-d-id/1338051?&web_view=true)
- **Office 365 phishing baits business owners with relief payments**  
[https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-business-owners-with-relief-payments/?&web\\_view=true](https://www.bleepingcomputer.com/news/security/office-365-phishing-baits-business-owners-with-relief-payments/?&web_view=true)
- **New 'Thanos' ransomware weaponizes RIPlace evasion technique**  
[https://searchsecurity.techtarget.com/news/252484469/New-Thanos-ransomware-weaponizes-RIPlace-evasion-technique?&web\\_view=true](https://searchsecurity.techtarget.com/news/252484469/New-Thanos-ransomware-weaponizes-RIPlace-evasion-technique?&web_view=true)
- **Average cost of DNS attacks hovering around \$924,00**  
[https://www.helpnetsecurity.com/2020/06/11/average-cost-of-dns-attacks/?&web\\_view=true](https://www.helpnetsecurity.com/2020/06/11/average-cost-of-dns-attacks/?&web_view=true)
- **Two code execution vulnerabilities in Microsoft Excel**  
[https://blog.talosintelligence.com/2020/06/vuln-spotlight-excel-code-execution-june-2020.html?&web\\_view=true](https://blog.talosintelligence.com/2020/06/vuln-spotlight-excel-code-execution-june-2020.html?&web_view=true)

- **Fake COVID-19 Contact-Tracing Apps Infect Android Phones**  
[https://www.darkreading.com/vulnerabilities---threats/fake-covid-19-contact-tracing-apps-infect-android-phones/d/d-id/1338047?&web\\_view=true](https://www.darkreading.com/vulnerabilities---threats/fake-covid-19-contact-tracing-apps-infect-android-phones/d/d-id/1338047?&web_view=true)
- **Cost of US Cyber Command Program Quintuples**  
[https://www.infosecurity-magazine.com/news/cost-of-us-cyber-command-program/?&web\\_view=true](https://www.infosecurity-magazine.com/news/cost-of-us-cyber-command-program/?&web_view=true)
- **Remote code execution vulnerability in Firefox's SharedWorkerService function**  
[https://blog.talosintelligence.com/2020/06/vuln-spotlight-firefox-shared-service-june-2020.html?&web\\_view=true](https://blog.talosintelligence.com/2020/06/vuln-spotlight-firefox-shared-service-june-2020.html?&web_view=true)
- **Tencent floats bug bounties for its cloudy Linux and IoT OSes**  
[https://www.theregister.com/2020/06/11/tencent\\_bug\\_bounties/?&web\\_view=true](https://www.theregister.com/2020/06/11/tencent_bug_bounties/?&web_view=true)
- **When Your Biggest Security and Privacy Threats Come From the Ones You Love**  
[https://www.darkreading.com/risk/when-your-biggest-security-and-privacy-threats-come-from-the-ones-you-love/d/d-id/1338053?&web\\_view=true](https://www.darkreading.com/risk/when-your-biggest-security-and-privacy-threats-come-from-the-ones-you-love/d/d-id/1338053?&web_view=true)
- **Babylon Health 'glitch' allowed app users access to others' video consults**  
[https://www.scmagazine.com/home/security-news/babylon-health-glitch-allowed-app-users-access-to-others-video-consults/?&web\\_view=true](https://www.scmagazine.com/home/security-news/babylon-health-glitch-allowed-app-users-access-to-others-video-consults/?&web_view=true)
- **Old insecure tech from turn of millennium still haunts 5G networks**  
[https://www.theregister.co.uk/2020/06/10/5g\\_gtp\\_flaws/?&web\\_view=true](https://www.theregister.co.uk/2020/06/10/5g_gtp_flaws/?&web_view=true)
- **Jenkins team avoids security disaster after partial user database loss**  
[https://www.zdnet.com/article/jenkins-team-avoids-security-disaster-after-partial-user-database-loss/?&web\\_view=true](https://www.zdnet.com/article/jenkins-team-avoids-security-disaster-after-partial-user-database-loss/?&web_view=true)
- **Slovak police seize wiretapping devices connected to government network**  
[https://www.zdnet.com/article/slovak-police-seize-wiretapping-devices-connected-to-government-network/?&web\\_view=true](https://www.zdnet.com/article/slovak-police-seize-wiretapping-devices-connected-to-government-network/?&web_view=true)
- **Financial and Economic Crime Targeted by New Europol Center**  
[https://www.govinfosecurity.com/financial-economic-crime-targeted-by-new-europol-center-a-14411?&web\\_view=true](https://www.govinfosecurity.com/financial-economic-crime-targeted-by-new-europol-center-a-14411?&web_view=true)
- **The Telehealth Attack Surface**  
[https://www.darkreading.com/endpoint/the-telehealth-attack-surface/a/d-id/1338019?&web\\_view=true](https://www.darkreading.com/endpoint/the-telehealth-attack-surface/a/d-id/1338019?&web_view=true)
- **Encryption Utility Firm Accused of Bundling Malware Functions in Product**  
[https://threatpost.com/legitimate-italian-guloder-obfuscator/156443/?&web\\_view=true](https://threatpost.com/legitimate-italian-guloder-obfuscator/156443/?&web_view=true)
- **QNAP NAS Devices Under Attack - Another Wave of eCh0raix Ransomware Identified**  
<https://cyware.com/news/qnap-nas-devices-under-attack-another-wave-of-ech0raix-ransomware-identified-7b1919c2>
- **Have You Received a VPN Configuration Notification? It's Fake!**  
<https://cyware.com/news/have-you-received-a-vpn-configuration-notification-its-fake-d483ccc2>
- **Your DNS Security Could be at Risk**  
<https://cyware.com/news/your-dns-security-could-be-at-risk-07268d0f>
- **Critical Vulnerability Patched in SAP Commerce**  
[https://www.securityweek.com/critical-vulnerability-patched-sap-commerce?&web\\_view=true](https://www.securityweek.com/critical-vulnerability-patched-sap-commerce?&web_view=true)
- **Hackers breached A1 Telekom, Austria's largest ISP**  
[https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/?&web\\_view=true](https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/?&web_view=true)
- **Google Warns of Emerging #COVID19 Cyber-Threat Hotspots**  
[https://www.infosecurity-magazine.com/news/google-warns-covid19-cyberthreat/?&web\\_view=true](https://www.infosecurity-magazine.com/news/google-warns-covid19-cyberthreat/?&web_view=true)
- **Microsoft discovers cryptomining gang hijacking ML-focused Kubernetes clusters**  
[https://www.zdnet.com/article/microsoft-discovers-cryptomining-gang-hijacking-ml-focused-kubernetes-clusters/?&web\\_view=true](https://www.zdnet.com/article/microsoft-discovers-cryptomining-gang-hijacking-ml-focused-kubernetes-clusters/?&web_view=true)
- **Criminals develop DDoS protection to stay online when rivals or law enforcement attack**  
[https://www.scmagazineuk.com/criminals-develop-ddos-protection-stay-online-when-rivals-law-enforcement-attack/article/1686079?&web\\_view=true](https://www.scmagazineuk.com/criminals-develop-ddos-protection-stay-online-when-rivals-law-enforcement-attack/article/1686079?&web_view=true)
- **Hackers took just three days to find a fake industrial network and fill it with malware**  
[https://www.zdnet.com/article/ransomware-hackers-took-just-three-days-to-find-this-fake-industrial-network-and-fill-it-with-malware/?&web\\_view=true](https://www.zdnet.com/article/ransomware-hackers-took-just-three-days-to-find-this-fake-industrial-network-and-fill-it-with-malware/?&web_view=true)
- **Gamaredon hackers use Outlook macros to spread malware to contacts**  
[https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/?&web\\_view=true](https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/?&web_view=true)
- **Attack Surface Area Larger Than Most Businesses Believe**  
<https://www.darkreading.com/perimeter/attack-surface-area-larger-than-most-businesses-believe/d/d-id/1338057>
- **Bad habits and risky behaviors put corporate data at risk**  
<https://www.helpnetsecurity.com/2020/06/11/risky-behaviors-put-corporate-data-at-risk/>
- **Top security risks for companies to address as cloud migration accelerates**  
<https://www.helpnetsecurity.com/2020/06/11/cloud-migration-risks/>
- **Congress wants to know what commercial spyware other countries are using**  
<https://www.zdnet.com/article/congress-wants-to-know-what-commercial-spyware-other-countries-are-using/>

## FRIDAY 12<sup>th</sup> May 2020

- **Honda resumes production at plants hit by suspected cyber attack**  
<https://in.reuters.com/article/honda-cyber/honda-resumes-production-at-plants-hit-by-suspected-cyber-attack-idINKBN23JOMJ>
- **CBI books PNB officials, private company employees over alleged loan fraud in Odisha**  
<https://www.hindustantimes.com/india-news/cbi-books-pnb-officials-private-company-employees-over-alleged-loan-fraud-in-odisha/story-XWyEM2qPh03INbJZLz37qK.html>
- **Encryption: a double-edged sword – EU law protections simultaneously impeding cross-border serious crime investigations?**  
<https://eulawlive.com/6324-2/>
- **American Cops Could Learn a Lesson From Italy's Carabinieri**  
<https://rusi.org/in-the-news/american-cops-could-learn-lesson-italy's-carabinieri>
- **Privacy: Google warns of COVID-19 related malware, phishing and spam**  
<https://gdpr.report/news/2020/06/12/privacy-google-warns-of-covid-19-related-malware-phishing-and-spam/>
- **Ransomware drives cyber insurers' loss ratio up 10pc**  
<https://www.cirmagazine.com/cir/2020061201.php>
- **Car auction bitcoin scam gang plead guilty to conspiracy**  
<https://portswigger.net/daily-swig/car-auction-bitcoin-scam-gang-plead-guilty-to-conspiracy>
- **Hackers are quick to notice exposed Elasticsearch servers**  
<https://www.bleepingcomputer.com/news/security/hackers-are-quick-to-notice-exposed-elasticsearch-servers/>
- **D-Link leaves severe security bugs in home router unpatched**  
<https://www.bleepingcomputer.com/news/security/d-link-leaves-severe-security-bugs-in-home-router-unpatched/>
- **Fraudster gets maximum jail time for news site DDoS extortion**  
<https://www.bleepingcomputer.com/news/security/fraudster-gets-maximum-jail-time-for-news-site-ddos-extortion/>
- **Coronavirus: Twitter removes more than 170,000 pro-China accounts**  
<https://www.bbc.co.uk/news/business-53018455>
- **Outrage over police brutality has finally convinced Amazon, Microsoft, and IBM to rule out selling facial recognition tech to law enforcement. Here's what's going on.**  
<https://www.businessinsider.com/amazon-microsoft-ibm-halt-selling-facial-recognition-to-police-2020-6?r=US&IR=T>
- **Zoom's crackdown on Chinese dissidents shows the price tech companies pay to operate in authoritarian countries**  
<https://www.businessinsider.com/zoom-china-crackdown-tech-firms-work-authoritarian-states-2020-6?r=US&IR=T>
- **Gamaredon hackers use Outlook macros to spread malware to contacts**  
[https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/?&web\\_view=true](https://www.bleepingcomputer.com/news/security/gamaredon-hackers-use-outlook-macros-to-spread-malware-to-contacts/?&web_view=true)
- **ICS Threat Snake Ransomware Suspected in Honda Attack**  
[https://www.darkreading.com/attacks-breaches/ics-threat-snake-ransomware-suspected-in-honda-attack/d/d-id/1338075?&web\\_view=true](https://www.darkreading.com/attacks-breaches/ics-threat-snake-ransomware-suspected-in-honda-attack/d/d-id/1338075?&web_view=true)
- **Deep Analysis of a QBot Campaign**  
[https://www.fortinet.com/blog/threat-research/deep-analysis-of-a-qbot-campaign-part-1?&web\\_view=true](https://www.fortinet.com/blog/threat-research/deep-analysis-of-a-qbot-campaign-part-1?&web_view=true)
- **A Bug in Facebook Messenger for Windows Could've Helped Malware Gain Persistence**  
[https://thehackernews.com/2020/06/facebook-malware-persistence.html?&web\\_view=true](https://thehackernews.com/2020/06/facebook-malware-persistence.html?&web_view=true)
- **New Android Spyware ActionSpy Revealed via Phishing Attacks from Earth Empusa**  
[https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/?&web\\_view=true](https://blog.trendmicro.com/trendlabs-security-intelligence/new-android-spyware-actionspy-revealed-via-phishing-attacks-from-earth-empusa/?&web_view=true)
- **Police Officers' Personal Info Leaked Online**  
[https://www.securityweek.com/ap-exclusive-police-officers-personal-info-leaked-online?&web\\_view=true](https://www.securityweek.com/ap-exclusive-police-officers-personal-info-leaked-online?&web_view=true)
- **Tor2Mine Refreshes Cryptomining Campaign Along With New Information Stealing Malware**  
[https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and\\_11.html?&web\\_view=true](https://blog.talosintelligence.com/2020/06/tor2mine-is-up-to-their-old-tricks-and_11.html?&web_view=true)
- **Researchers Discover Privilege Escalation Vulnerability in Windows 10 Platform**  
[https://www.fortinet.com/blog/threat-research/fortiguard-labs-security-researcher-discovers-privilege-escalation-vulnerability-in-windows-platform?&web\\_view=true](https://www.fortinet.com/blog/threat-research/fortiguard-labs-security-researcher-discovers-privilege-escalation-vulnerability-in-windows-platform?&web_view=true)
- **MAZE Attacks Victoria Beckham's Advisory Firm**  
[https://www.infosecurity-magazine.com/news/maze-attacks-victoria-beckhams/?&web\\_view=true](https://www.infosecurity-magazine.com/news/maze-attacks-victoria-beckhams/?&web_view=true)
- **Lawsuit Filed Against Accounting Firm in Patient Data Hack**  
[https://www.inforisktoday.com/lawsuit-filed-against-accounting-firm-in-patient-data-hack-a-14423?&web\\_view=true](https://www.inforisktoday.com/lawsuit-filed-against-accounting-firm-in-patient-data-hack-a-14423?&web_view=true)
- **Researchers Detect Largest Account Takeover Attack on Online Banking Service**  
[https://www.imperva.com/blog/imperva-takes-on-its-largest-recorded-account-takeover-attack-on-a-single-company/?&web\\_view=true](https://www.imperva.com/blog/imperva-takes-on-its-largest-recorded-account-takeover-attack-on-a-single-company/?&web_view=true)
- **Unsecured AWS S3 Buckets Infected With Skimmer Code**  
[https://www.govinfosecurity.com/unsecured-aws-s3-buckets-infected-skimmer-code-a-14421?&web\\_view=true](https://www.govinfosecurity.com/unsecured-aws-s3-buckets-infected-skimmer-code-a-14421?&web_view=true)
- **Authorities Probe Radio, Website Disruptions During Protests**  
[https://www.securityweek.com/authorities-probe-radio-website-disruptions-during-protests?&web\\_view=true](https://www.securityweek.com/authorities-probe-radio-website-disruptions-during-protests?&web_view=true)

- **Twitter bans 32k accounts pushing Chinese, Russian, and Turkish propaganda**  
[https://www.zdnet.com/article/twitter-bans-32k-accounts-pushing-chinese-russian-and-turkish-propaganda/?&web\\_view=true](https://www.zdnet.com/article/twitter-bans-32k-accounts-pushing-chinese-russian-and-turkish-propaganda/?&web_view=true)
- **Vulnerability in Mitsubishi Controllers Can Allow Hackers to Disrupt Production**  
[https://www.securityweek.com/vulnerability-mitsubishi-controllers-can-allow-hackers-disrupt-production/?&web\\_view=true](https://www.securityweek.com/vulnerability-mitsubishi-controllers-can-allow-hackers-disrupt-production/?&web_view=true)
- **Russia says Germany has not provided any evidence of Bundestag hack**  
[https://www.zdnet.com/article/russia-says-germany-has-not-provided-any-evidence-of-bundestag-hack/?&web\\_view=true](https://www.zdnet.com/article/russia-says-germany-has-not-provided-any-evidence-of-bundestag-hack/?&web_view=true)
- **City Pays Ransom Despite Pre-Ransomware Outbreak Hack Alert**  
[https://www.govinfosecurity.com/city-pays-ransom-despite-pre-ransomware-outbreak-hack-alert-a-14427?&web\\_view=true](https://www.govinfosecurity.com/city-pays-ransom-despite-pre-ransomware-outbreak-hack-alert-a-14427?&web_view=true)
- **Six New Vulnerabilities Found on D-Link Home Routers**  
[https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/?&web\\_view=true](https://unit42.paloaltonetworks.com/6-new-d-link-vulnerabilities-found-on-home-routers/?&web_view=true)
- **COVID-19 scams could be targeting stimulus payments, according to IRS**  
[https://www.ibtimes.co.uk/covid-19-scams-could-targeting-stimulus-payments-according-irs-1679491?&web\\_view=true](https://www.ibtimes.co.uk/covid-19-scams-could-targeting-stimulus-payments-according-irs-1679491?&web_view=true)
- **CrossTalk - Another Intel-Exclusive Vulnerability Worries Security Researchers**  
<https://cyware.com/news/crosstalk-another-intel-exclusive-vulnerability-worries-security-researchers-a39bc2fe>
- **Just a Wink and Smile - the Avaddon Pathway to Doom**  
<https://cyware.com/news/just-a-wink-and-smile-the-avaddon-pathway-to-doom-5aac64f8>
- **Over 100,000 UK Security Cameras Could Be at Risk of Hacking**  
[https://www.infosecurity-magazine.com/news/uk-security-cameras-risk-hacking/?&web\\_view=true](https://www.infosecurity-magazine.com/news/uk-security-cameras-risk-hacking/?&web_view=true)
- **Hacker Bypasses GE's Ridiculous Refrigerator DRM**  
[https://www.vice.com/en\\_us/article/jgxpjy/hacker-bypasses-ges-ridiculous-refrigerator-drm?&web\\_view=true](https://www.vice.com/en_us/article/jgxpjy/hacker-bypasses-ges-ridiculous-refrigerator-drm?&web_view=true)
- **15 Individuals Plead Guilty to Multimillion-Dollar Online Auction Fraud Scheme**  
<https://www.darkreading.com/attacks-breaches/15-individuals-plead-guilty-to-multimillion-dollar-online-auction-fraud-scheme/d/d-id/1338082>
- **Canadian cryptocurrency firm collapsed due to Ponzi scheme by late founder, regulator says**  
<https://www.reuters.com/article/us-crypto-currencies-quadriga/canadian-cryptocurrency-firm-collapsed-due-to-ponzi-scheme-by-late-founder-regulator-says-idUSKBN23I3AF>
- **Italians embrace coronavirus tracing app as privacy fears ease**  
<https://www.reuters.com/article/us-health-coronavirus-italy-apps/italians-embrace-coronavirus-tracing-app-as-privacy-fears-ease-idUSKBN23I2M5>
- **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/>
- **Contact-tracing apps might not work in some busy city environments**  
<https://www.zdnet.com/article/contact-tracing-apps-might-not-work-in-some-busy-city-environments/>

[End]

The contents of this report are all taken from 3<sup>rd</sup> 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