ABOUT
ACCUME PARTNERS

Accume Partners is a trusted advisor that serves clients by delivering integrated Risk, Regulatory, and Cybersecurity solutions to help manage uncertainty and drive business value.

Bob Gaines
Director
Cybersecurity & Privacy
425-518-1914
rgaines@accumepartners.com

May 22nd, 2020

accume partners

COVID-19 SECURITY NEWS

Covid-19
Security News

Cybercriminals Target U.S. Citizens for COVID-19 Stimulus Fraud. On March 27, 2020, the U.S. government approved a $2 trillion USD stimulus package that provides COVID-19 (also known as coronavirus) pandemic relief for qualified taxpayers in the form of $1,200 checks. Since then, Secureworks® Counter Threat Unit™ (CTU) researchers have observed an increase in tax identity theft aimed at fraudulently obtaining stimulus checks. In another underground forum post, an English-speaking threat actor known as "DoctorZempf" claimed to have found information by searching tax preparers' trash dumpsters. Cybercriminals could use taxpayer information to steal identities and apply for a victim's stimulus relief check.

Source: https://www.secureworks.com/blog/cybercriminals-target-us-citizens-for-covid-19-stimulus-fraud

Surge in security concerns due to remote working during COVID-19 crisis. As people settle into the new way of working with many organizations working from home, it comes as no surprise that attention now turns to being productive as well as secure. In a recent survey, Barracuda found that almost half (46%) of global businesses have encountered at least one cybersecurity scare since shifting to a remote working model during the COVID-19 lockdown. What's more, an astounding 49 percent say they expect to see a data breach or cybersecurity incident in the next month due to remote working.

Source: https://blog.barracuda.com/2020/05/06/surge-in-security-concerns-due-to-remote-working-during-covid-19-crisis/

Coronavirus-related cyberattacks surge to 192,000 in one week. As the coronavirus outbreak has expanded around the world so too have cyberattacks designed to take advantage of the disease. Cybercriminals have been creating phishing emails, suspicious websites, downloadable apps and files, and other malicious content all geared toward trapping people curious or anxious about the pandemic. A blog post published Tuesday by cyber threat intelligence provider Check Point Research illustrates the rise of certain types of coronavirus-related cyberattacks.

Source: https://www.techrepublic.com/article/coronavirus-related-cyberattacks-surge-to-192000-in-one-week/

COVID-19 blamed for 238% surge in cyberattacks against banks. On Thursday, VMware Carbon Black released the third edition of the Modern Bank Heists report, which says that financial organizations experienced a massive uptick in cyberattack attempts between February and April this year -- the same months in which COVID-19 began to spread rapidly across the globe. The cybersecurity firm's research, which includes input from 25 CIOS at major financial institutions, adds that 80% of firms surveyed have experienced more cyberattacks over the past 12 months, an increase of 13% year-over-year.

Source: https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/