EINPRESSWIRE

Cybersecurity Expert Ian Marlow Discusses How Cyber Crimes Increased In 2020 and 2021

Cybersecurity expert Ian Marlow recently discussed how cyber crimes have increased in the past two years.

Cybersecurity expert Ian Marlow

BOCA RATON, FL, FL, USA, July 30, 2021 /EINPresswire.com/ -- The COVID-19 pandemic took more people online than ever before. This created new opportunities for many, including cybercriminals. Cybersecurity expert Ian Marlow recently discussed how cyber crimes have increased since the COVID-19 pandemic took hold.

"The COVID-19 pandemic increased uncertainty about the economy as well as everyday life," Ian Marlow said. "The exploitation of this fear, alongside an increased online presence, made circumstances that were ideal for cybercriminals."

Ian Marlow explained numerous types of cyber crimes have increased over the past two years, including phishing, online scams, malicious domains, data harvesting malware, and misinformation. Unfortunately, the fight against cybercriminals has not decreased as the pandemic has begun to subside.
"We will likely see cyber crimes continuing to increase throughout the immediate future," Ian Marlow said. "People are still working from home, which has created a long list of new vulnerabilities. This combined with increased activity by cybercriminals is keeping us in the cybersecurity field on high alert for as long as we can tell."

Marlow stated that the COVID-19 vaccine does not mark an end or decrease in cybercrimes. This is because an entirely new round of phishing related to the vaccine and medical products will likely be created. These attacks are used as ways to steal important personal and company data.

> The COVID-19 pandemic increased uncertainty about the economy as well as everyday life”
>
> *Ian Marlow*

Ian Marlow added that many businesses have seen financial benefits from employees working from home. Many employees are continuing to work remotely or in a hybrid of at-home and at-office work. This substantially increases remote work from inside and outside the corporate network. It also means bringing your own devices, which can bring about other cybersecurity issues.

This means they will likely continue functioning in this format or with several work-at-home days per week. Marlow suggested cybercriminals will continue to develop more ways to attack these work-at-home systems.

"It has been stated that cybercriminals were able to ransom businesses for millions of dollars throughout the pandemic so far," Marlow said. "They're using the same tactics they've used for decades now; phishing, hacking, social engineering, and more."

Marlow concluded that it pays for companies to focus on increasing cybersecurity now and in the coming years. Data breaches during the pandemic averaged $21,659 for a single incident, with 5 percent of incidents reaching $1 million or higher.

"There's no better time than now to hire a cybersecurity expert to ensure your line of defense is up-to-date," Ian Marlow finished. "Invest in educating your workforce and in updated cybersecurity technologies to protect yourself, your employees, and your bottom line.

Caroline Hunter
Web Presence, LLC
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/547657791