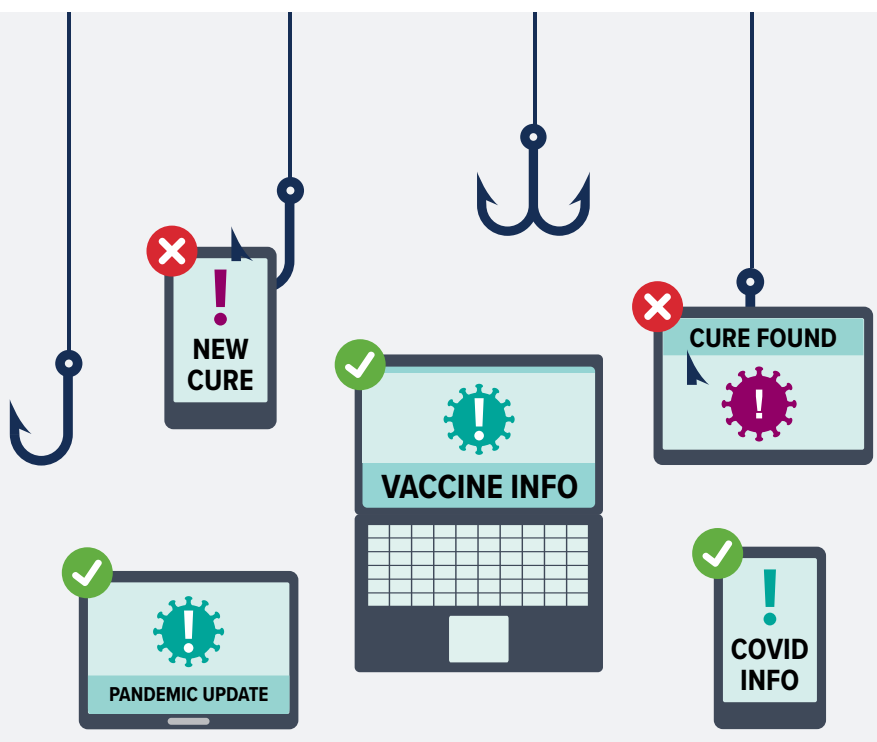
2021 Cybersecurity Predictions

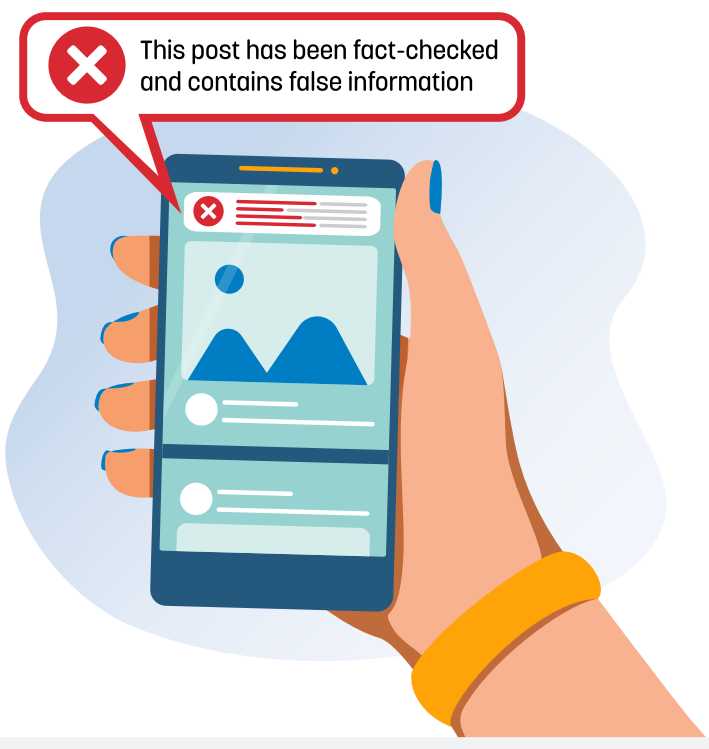
We'll see the consequences of employees letting their guards down as work-from-home extends.

Bad actors will seek to take advantage of workers who have been remote since the start of the pandemic, as they may be more likely to be letting down their guard when it comes to following security protocols. Combined with threats that already exist in a rushed remote work environment, this will result in data loss rates exceeding what we saw in 2020.

Attackers will use the COVID-19 vaccine to conduct the largest phishing effort of the year.

In 2020, hackers used COVID-19 to fuel a plethora of phishing scams. The number of legitimate emails sent on the topic allowed phishing emails to hide in plain sight. As the race to distribute a vaccine continues, people will once again seek information on new developments. The amount of content plus the thirst for knowledge will set the stage for another spike in phishing attacks.



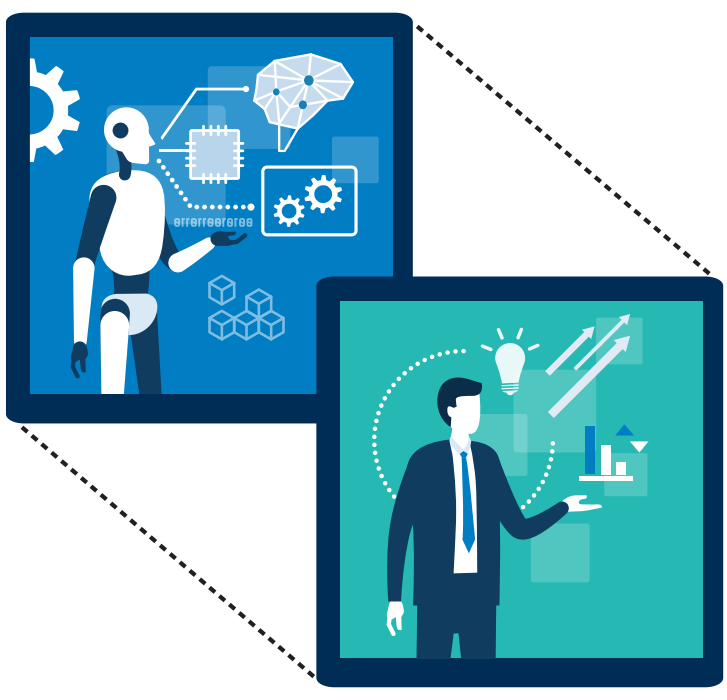


We will see a rise in internet policing as misinformation reaches new heights following the U.S. elections.

In the wake of rampant misinformation during the 2020 U.S. election, fear of further escalation will lead to a call for tighter protocols on the internet, including federal legislation enforcing better safeguards among tech and media giants. 2021 will be a year of holding these organizations accountable using regulation versus allowing them to "self-police."

The board meeting of a major company conducted using video conferencing software will be exposed, resulting in a high-profile scandal.

With so much of the world staying at home and finding new ways to communicate with others, people are using collaboration tools for everything, including confidential discussions. As threat actors continue to become more sophisticated, we will see one gain access to a public company's board meeting and leak compromising business information that results in a high-profile scandal.



Deepfakes will become a significant threat to business integrity.

ThisPersonDoesNotExist.com demonstrates just how little information hackers need to create sophisticated deepfakes. And with the rise in video conferencing technology — which have employees' names and pictures automatically associated with them — they'll create convincing fakes of leaders to exploit employees internally for financial gain and to manipulate the public externally into thinking the CEO of a public company has done something damaging.

There will be a reckoning within the growing API security market as API data breaches rise.

APIs are one of the largest attack surfaces for organizations, with more and more businesses across industries building out microservices that use APIs. However, very few companies know how to build them securely, and the growing API security market is beginning to falter. This will result in a high-level breach and data loss that will be directly traced back to unsecured APIs.