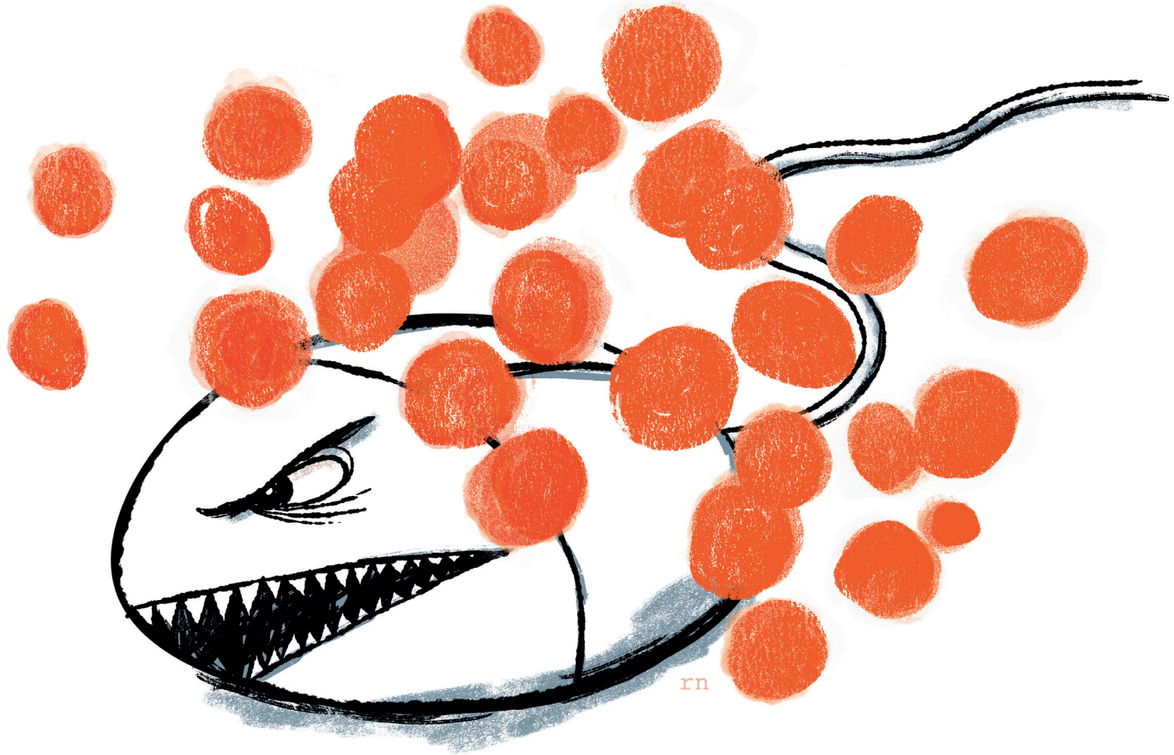
By Brunswick's
**SIOBHAN GORMAN** and
**YASMIN BROOKS**



# HACKERS Exploit the Pandemic

Within weeks of the COVID-19 coronavirus outbreak, hackers have already commandeered the virus to unleash cyberattacks, sending emails purporting to provide coronavirus guidance laced with cyberattack software. In one more alarming case, they appear to have attacked a hospital and forced it to cancel operations and take key systems offline.

As the outbreak continues to intensify, the UK National Cyber Security Centre (NCSC) warned that the volume of these attacks will likely increase, pointing to the increased registration of coronavirus-related webpages.

Criminals are opportunists, and the Covid-19 global onslaught has brought with it not just health threats but cybersecurity risks, too. As companies move to protect the health of their workforce, it's also important to protect the systems they're using to run their businesses.

It's especially important for hospitals to shore-up their cyberdefenses. If they don't, just as they are racing to respond to Covid-19, they could face situations like University Hospital Brno in the Czech Republic, which earlier this month was forced to divert patients and cancel planned operations while it worked to address an attack.

The most likely cyber threats are email "phishing" campaigns that use the coronavirus as a lure to get the recipient to open an attachment that contains malware. According to the NCSC, such "phishing" attempts are happening on a global scale in multiple countries, which has led to both a theft of money and sensitive data.

Similarly, known hacker groups have been launching websites purporting to sell masks or other safety-related measures for coronavirus, possibly to use them as another vector for cyberattacks.

The NCSC has also cautioned that these attacks are "versatile and can be conducted through various media, adapted to different sectors and monetized via multiple means, including ransomware, credential theft, bitcoin or fraud."

The cybersecurity firm ProofPoint has seen a rise in these cyberattack emails with Covid-19 themes since January. Both ProofPoint and IBM's X-Force cybersecurity unit identified a campaign that targeted users in Japan with an email masquerading as a coronavirus information email that carries with it a potent type of cybercrime software.

In the US, the Secret Service recently warned of scams from online criminals posing as sellers of high-demand medical supplies to prevent coronavirus. They'll require payment upfront and not send the products.

Cyber criminals have also been posing as the World Health Organization and the US Centers for Disease Control and Prevention (CDC), sending fraudulent emails from the former and "creating domain names similar to the CDC's web address to request passwords and even bitcoin donations to fund a vaccine" for the latter.

In addition to the use of the coronavirus as a cyberattack vector, the growing need for working remotely to mitigate the spread of Covid-19 has increased companies' exposure to cyber threats. The increase in remote work creates more opportunities for hackers to make inroads from less secure locations.

Companies should also ensure they can provide adequate security when their whole workforce is remote. They should quickly work through the security implications of workers choosing to switch to insecure personal devices. With national-level pressures on home broadband, staff will also resort to mobile hotspots, which are often less secure. And enabling remote connectivity at scale, with the right security configurations, can be a challenge even with months of preparation time.

A recent US Department of Homeland Security Covid-19 cybersecurity notice pointed to the importance of making sure that security measures are up to date for companies' remote access systems. Additional measures to consider include enabling multifactor authentication—which can require two or more steps to verify a user's identity before granting access to corporate networks. The NCSC is also working to identify malicious sites responsible for phishing and cyberattack software.

A final looming cyberthreat related to Covid-19 is disinformation. The World Health Organization and other agencies have for months been combatting disinformation campaigns spreading false information about the origins of and treatments for Covid-19—reports that seed more confusion and increase risks to society.

All of that means that computer virus risks are emerging as the biological virus spreads—and both are a threat to business. Cyber risk mitigation efforts should account for the different ways that a company can be affected, including impacts on the technical, operational, legal and reputational aspects of a business. Often, the reputational effects of a cyberattack are more significant than direct the business or technical impact.

To mitigate all of the potential impacts of cyberattacks taking advantage of the Covid-19 outbreak, companies should:

- Review and update crisis and cybersecurity response plans, and ensure internal and external communications response plans are robust.
- Confirm that members of the crisis management team understand their roles and responsibilities.
- Make sure all communications channels have the latest security patches.
- Review and update access controls, particularly when remote access is used heavily, to make sure that only those who require access to sensitive systems to do their jobs have it.
- Take extra care when handling medical information. For companies managing employees who have contracted Covid-19, it's important that personal health information is handled with strong security measures, including encryption.
- Educate employees about the cyber risks that may attempt to capitalize on fear of the Covid-19 virus—whether it be phishing email or disinformation.

Covid-19 poses a number of short- and long-term challenges to business resilience, and the virus's trajectory is quick and unpredictable. But it's possible to anticipate and mitigate a number of the cyber threats that will try to ride the virus's coattails. The companies that do will be more resilient and better positioned to withstand the direct health and operational effects of the virus. ◆

**CRIMINALS ARE OPPORTUNISTS, AND THE COVID-19 GLOBAL ONSLAUGHT HAS BROUGHT WITH IT NOT JUST HEALTH THREATS BUT CYBERSECURITY RISKS, TOO.**

**SIOBHAN GORMAN** is a Partner in Brunswick's Washington, DC office and co-lead of the firm's Cybersecurity, Data, & Privacy Practice.
**YASMIN BROOKS** is a Director based in London.

ILLUSTRATION: ROBERT NUEBECKER