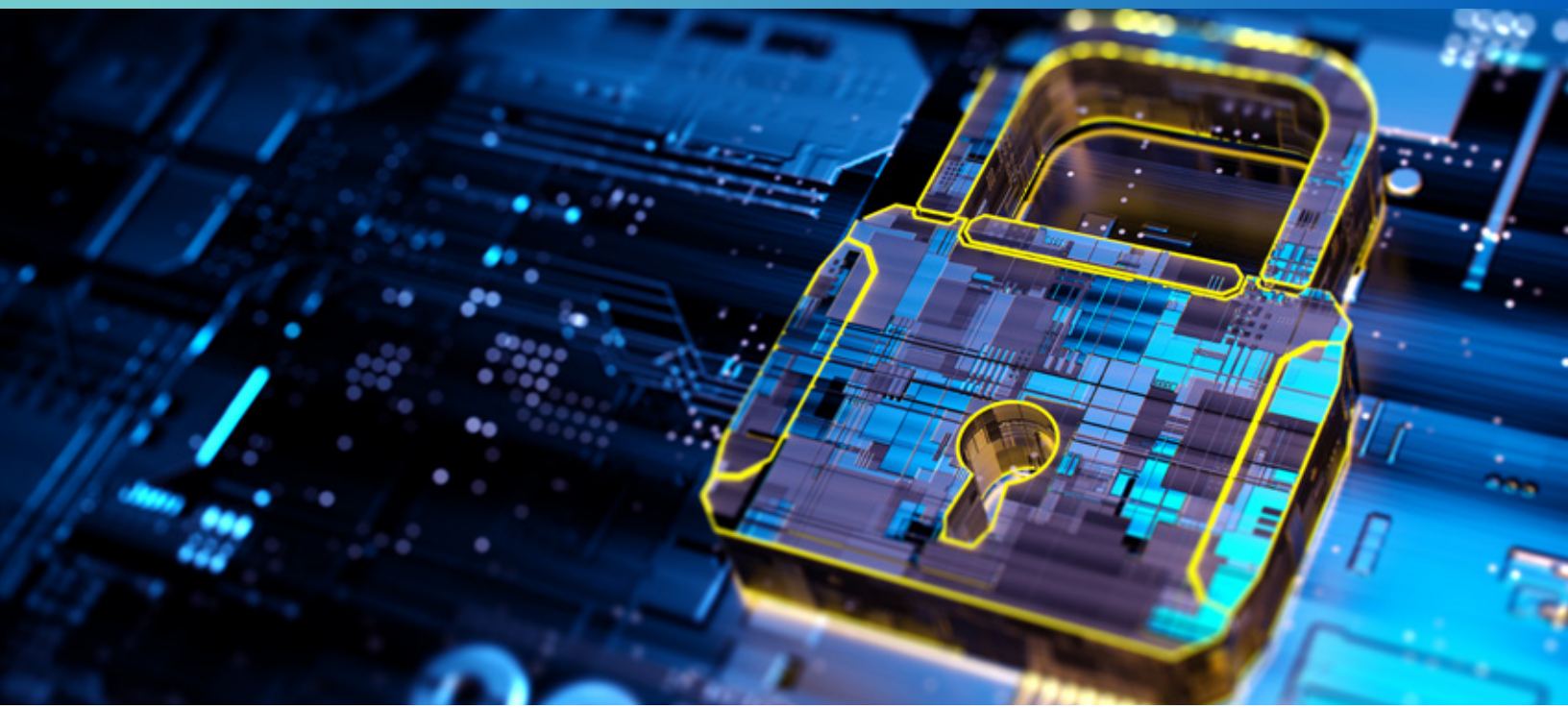

Secure Your Network and Stop Cybercriminals from Capitalizing on a Crisis

Part of the Driving Digital Agility content series: Insights and strategies to pivot to digital business, navigate new work environments, and manage changing customer expectations.

As businesses adapt to support a primarily remote workforce, they must also secure network connections to protect their people, assets, and customers from cybercriminals who consider the global circumstances an opportunity to prey on emotional and technical vulnerabilities across distributed work environments.

When businesses around the world changed the way they worked in response to COVID-19, cybercriminals ramped up their efforts to corrupt corporate networks with increased phishing, spoofing, distributed denial of service (DDoS), malware, and other malicious attacks.

Cybersecurity professionals must stave off almost constant attempts to breach network security in normal times. During a global crisis, the efforts from cybercriminals multiply exponentially as they seek to expose technical vulnerabilities and play on people's emotions. We need to look no further than our own data to see the prevalence of hacking attempts — about 87% of the 1.5 billion emails Comcast Business processes every year are some sort of phishing attempt to lure people to click through to a spoofing site where malware would download to their device. Since lockdowns began in mid-March, we've seen those numbers climb even higher.

"In the past six weeks, we have seen tens of thousands of new websites that try to exploit people's need to know and need to connect on topics related to COVID-19," says Noopur Davis, Executive Vice President, Chief Product and Information Security Officer, Comcast. "Our data shows on a typical day DDoS attacks have increased by 33% since COVID. The bad guys are using the same approaches—but at a much bigger scale and by exploiting our current vulnerabilities."

IT security leaders can protect personnel and environments by educating employees on what to avoid in emails and other communications, and by boosting security measures on the devices being used and the connections between remote employees and corporate networks.

The New Network Normal

"Comcast, in its residential networks, provides more than 30 million customer households with connectivity"

— Shena Tharnish, Vice President, Cybersecurity Products, Comcast Business

Unfortunately, when the world responded to COVID-19 by staying home, cybercriminals started working harder to find holes in corporate networks that are being stressed by remote work.

The types of attacks aren't different, but the volume of attempts is skyrocketing, particularly those that hope to exploit the vulnerabilities of people and the networks and devices they are using to do work. Phishing and spoofing efforts have increased and attackers are using terms like "COVID," "coronavirus," "test kits," and "vaccine" to lure people to click on links and visit websites. Once on the site, malware and ransomware could download to a device—later connecting to and infecting the broader company network.

"Comcast, in its residential networks, provides more than 30 million customer households with connectivity. We have a massive peering backbone and that's where we are seeing the biggest increase in DDoS," says Shena Seneca Tharnish, Vice President, Cybersecurity Products, Comcast Business. "We are also seeing a tremendous amount of growth in phishing with residential emails. The volume is mind-blowing, but the trends are the same."

For instance, John Hopkins University has, from the start of the crisis, provided worldwide reporting information on COVID-19. Websites have spun up posing as this reputable source, relying on people's need to know and posing a significant threat to visitors.

DDoS attacks are also on the rise. DDoS attacks attempt to make a machine or a network unavailable by flooding the machine with requests, which prevents legitimate requests from being fulfilled. "With DDoS, the attacker doesn't want people to be able to reach the site or be able to do work on a site," says Davis. "The goals with phishing are to download some sort of malware and ultimately steal credentials and commit fraud."

Securing a Distributed Workforce

Remote work is not new for most IT security professionals who have long enabled employees to access corporate resources via secure virtual private network (VPN) connections. However, the recent rush to remote work has stressed existing business networks and connections, which may not be designed to support the majority of their employees logging in remotely.

Security leaders must reassess how they make needed company resources available without increasing risk as many supported devices are not using secure private networks, but residential Internet to do their jobs. “In private business networks, there is a lot more control to ensure attacks can be stopped and human error can be caught. Now it is not safe to assume that the endpoints can be trusted to access the corporate networks,” says Tharnish.

“In private business networks, there is a lot more control to ensure attacks can be stopped and human error can be caught. Now it is not safe to assume that the endpoints can be trusted to access the corporate networks.”

— Shena Tharnish, Vice President, Cybersecurity Products, Comcast Business

There are several protections IT security leaders, either on their own or through the help of trusted partners, can put in place now to enable remote work while also reducing risk:

Secure VPN

By providing a VPN tunnel on either end of a connection between a residence and company assets, IT security pros can lessen the threat posed by devices connecting to their private network via the public Internet. This secure connection also provides visibility into the devices connected to the environment and can enable patching for security threats on distributed devices.

Zero trust

To be safe, a zero-trust framework assumes no trust in a network, device, or identity and requires those accessing resources to prove who they are. Zero trust also leverages identity and access management technologies to assign appropriate access permissions to everyone in the organization. For instance, an employee working in marketing wouldn’t need access to sensitive financial information used by someone in accounting.

Multi-factor authentication

Two-factor authentication is a subset of multi-factor authentication, which requires more than two pieces of evidence to authenticate that a person is who they say they are when logging in. For instance, some access requires entering a code sent to a specific user’s device after entering their username and password. By enabling multi-factor authentication, employers are able to prevent unwanted access, even after a hacker has obtained a user’s username and password.

Virtual Desktop Infrastructure

If the devices being used for work cannot be trusted, companies can use a virtual desktop infrastructure (VDI) to provide the needed resources to get work done without exposing the underlying network to the threats posed by unsecured devices. VDI, often available via cloud-based offerings, renders an image and doesn’t download actual data to the device, blocking off unnecessary access.

Securely Navigating the Pandemic

Superior IT security is a fundamental requirement for doing business in the digital age. COVID-19 forced many businesses to consider how they would support and now secure a mostly remote workforce that is unfortunately sensitive and vulnerable to malicious attacks and social engineering.

IT security professionals can prevent problems by educating end users on the dangers of clicking on links in emails or visiting unsafe websites. By resisting the urge to respond to phishing attempts, end users are helping to protect their business. Going forward, security leaders will need to build out their secure infrastructure in a way that enables secure connectivity and access, letting employees work from anywhere without worry.

To watch the Comcast Business "Keeping Cybercriminals at Bay—and Protecting Your Business—During a Crisis" webinar, **please click here**.

For more information on how businesses can use technology to navigate new work environments and expectations, explore the rest of our "Driving Digital Agility" blog series.

READ MORE

COMCAST BUSINESS