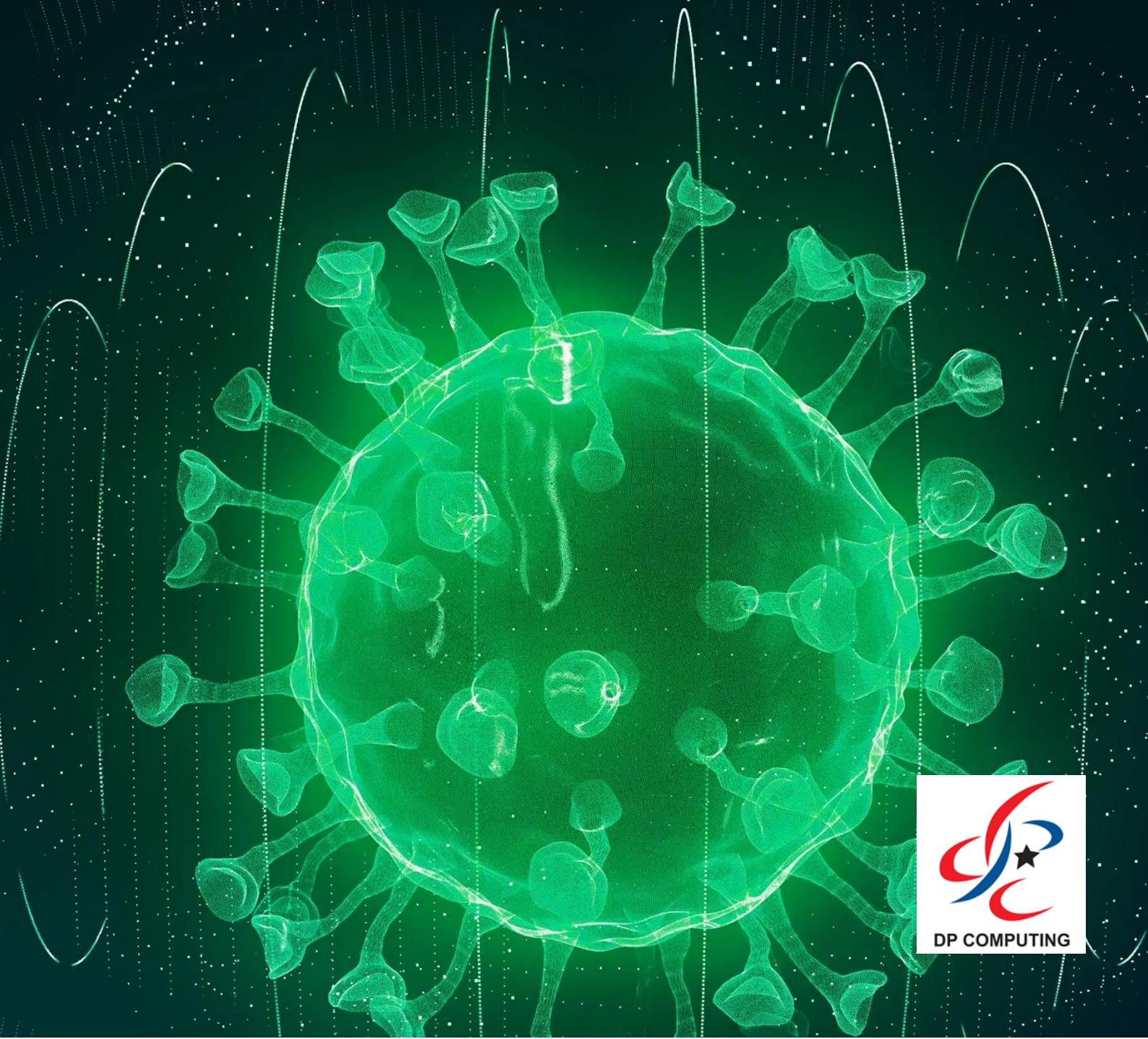
CYBER CREEPS AND COVID-19

BE WARY

OF THESE

I.T. THREATS



DP COMPUTING

INTRODUCTION

IT support technicians already has enough to worry about with COVID sending everyone home to work. Too bad cybercriminals are such opportunistic creeps as they are taking advantage of the global health pandemic to scam unsuspecting users. This eBook highlights many coronavirus-related scams. Be aware, so you can educate both yourself and your employees to best protect your business.

Email remains the number-one means of attack. Cybercriminals are increasingly sophisticated and are motivated by the dollar. Today, companies from any industry of any size can face a targeted threat.

Whether it is a phishing attack or a malicious attachment, these bad actors prey on human nature. They will target your staff's heightened fear and desire to help or tap into the near-Pavlovian response to urgency or a "steal of a deal." Right now, they are looking to benefit from the worldwide anxiety about the coronavirus pandemic. While businesses grapple with remote work processes, cybercriminals are finding new weaknesses.

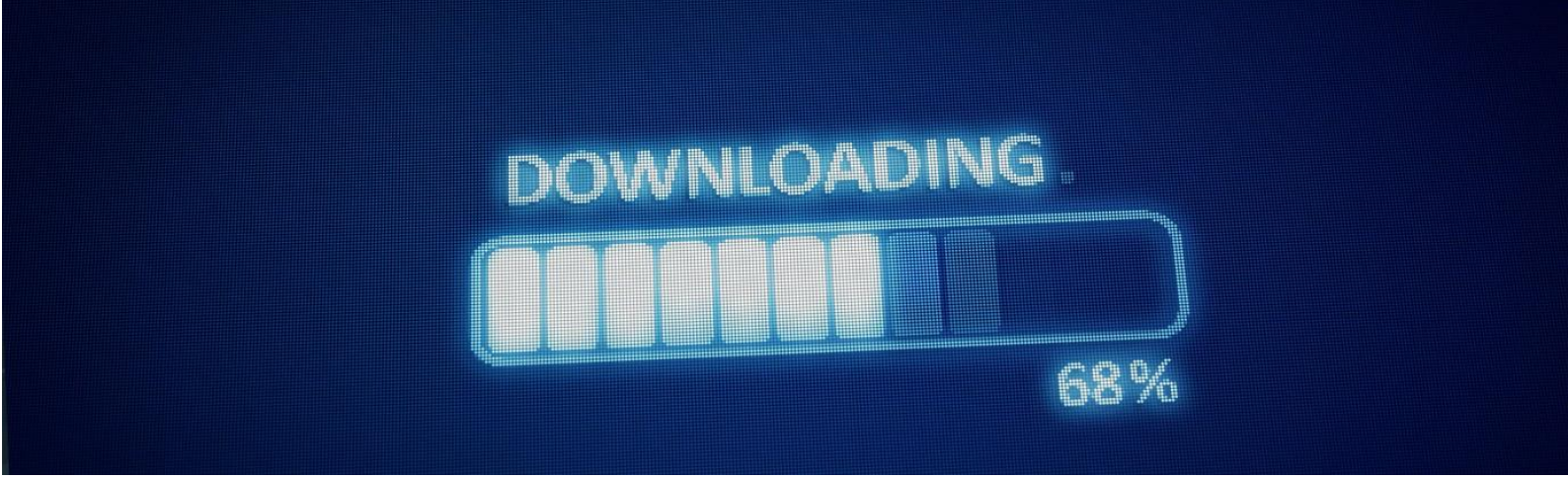
This roundup of known threats related to COVID-19 can help business owners plan and implement their businesses defences. We will also discuss the need to educate employees and then suggest a top solution for protecting your business email communications.

COVID-19 SCAMS OUT THERE

Cybercriminals are nimble crooks who capitalize on current events. As soon as there is a fresh news story or angle for their attacks, they adapt quickly. Right now, they are taking advantage of the coronavirus. As businesses change the way they work, bad actors see an opportunity to find new entry points for attack. They will try any means to phish for sensitive data, breach systems or deliver malware.

Scams are not new; it is a matter of how they are delivered. In the past, a Nigerian prince wanted to send you millions and now, governments are giving out money in the form of economic stimulus payments. The scammers jumped right in. Scam emails ask for bank information to pay relief funds directly, or the emails request other personal data you would not want to reveal to a criminal.

Fake bank, telephone, or insurance company phishing emails are another problem. These ask for personal and financial information, lure the user into opening malicious links or attachments, or seek remote access to the user's device. Emails impersonating healthcare organisations are also common. The CDC, WHO, and other healthcare organizations are not reaching out directly to individuals.



Downloading a “Safety Measures” document or the like could introduce malware or take an employee to a malicious site where a fake virus tracking app is set up to deliver malware. The ”COVID19 Tracker” app infects a device and demands $250 in Bitcoin. Emails offering fake news about someone infected in your local area are another tactic. Sometimes, cybercrooks target a business with a communication saying there’s a shipping problem caused by COVID. Notifying the recipient that a package is held up, the email encourages the user to click on a malicious file or link to remedy the problem.

Hackers are even gaining access to corporate mailboxes or relying on a close approximation to fool the busy reader. Then, they send links or attachments promising to outline a company coronavirus policy. Often, these will ask the user to log in to view the necessary documentation. If the user does not question the communication, hackers capture employee access information.

You don’t have to look at flexibility and security as a sliding scale. Digital technology balances both the need to accommodate work from home, and to protect business systems and networks.

EDUCATE YOURSELF

People are the foundation of your businesses success but at the same time, they can also represent a real security threat. According to Experian, only 45% of companies have mandatory cybersecurity training.

Yet you and your staff need to understand the many ways in which they can put the business at risk. Your IT consultants cannot be the only ones making cybersecurity a priority.

In educating employees about potential cybersecurity issues, you:

- Impress the importance of caution and questioning the source of any communication with links or attachments. Hovering over URLs can show where the link leads. Grammatical and spelling errors are often a red flag, too.

- Require installation of the latest malware, antivirus protections, and security patches.

- Explain why you have an acceptable-use policy. Talk about what could happen if they decide to download that one app from the Web to their work device.

- Warn them about installing random USB drives hoping to connect the stray device to its owner. Dropping thumb drive devices is a common way cybercriminals gain illicit access.

- Emphasize the importance of physical security, too. A stolen unencrypted laptop or an unknown person accessing an on-site computer can lead to a breach.

- Provide them with a way to report suspicious emails, communications, and potential compromise.

PROTECT YOUR BUSINESS

Even after you've taken the above advice to educate employees, there are still risks. Some of these emails are very convincing. People are busy, working fast, tired and overly trusting. Additionally, these particular scams are targeting our preoccupation and fears around the coronavirus.

Computer antivirus and other security systems can do its best, but it only takes one bad click to breach your system.

An email gateway is the best defence against email malware. This solution removes malicious files or links before they reach your employees' inboxes. A gateway scans all business emails for any signs of harmful content.

This can include scanning outbound and internal emails. Why would you want to do that? To protect yourself from data loss or compliance risks. For instance, gateway email archiving stores communications for later audits.

PROTECT YOUR BUSINESS

Secure email gateways provide protection by offering:

- spam filtering;
- virus and malware blocking;
- phishing protection;
- admin controls and reporting.

The email gateway collects different cloud-based technologies working together to block threats. Working as an extra layer of security, the gateway enforces rules about what email can enter or leave the network. As this is done on a network level, it also means the protection works on all devices, whether your staff are on-site or working remotely.

WE CAN HELP

Installing gateway email protection may be one more thing to add to an already extensive “to do” list but we can help. Contact our IT experts today and we can help your organization to stay cybersecure in these tumultuous times.

Adelaide, South Australia

Phone (08) 8326 4364

support@dpcomputing.com.au

www.dpcomputing.com.au

facebook.com/dpcomputing