COVID-19

Staying cyber secure

The COVID-19 pandemic is changing our lives. People are concerned, and with that concern comes a desire for information, safety and support. Organised crime groups are exploiting the fear, uncertainty and doubt which COVID-19 brings to target individuals and businesses in a variety of ways.

The threat

Since mid-February, KPMG member firms have seen the rapid build-out of infrastructure by cybercriminals used to launch COVID-19 themed spear-phishing attacks and to lure targets to fake websites seeking to collect Office 365 credentials.

Examples of campaigns mounted include:

- COVID-19 themed phishing emails attaching malicious Microsoft documents which exploit a known Microsoft vulnerability to run malicious code
- COVID-19 themed phishing emails attaching macro-enabled Microsoft word documents containing health information which trigger the download of Emotet or Trickbot malware
- Multiple phishing emails luring target users to fake copies of the Centre for Disease Control (CDC) website which solicit user credentials and passwords
- A selection of phony customer advisories purporting to provide customers with updates on service disruption due to COVID-19 and leading to malware download
- Phishing emails purporting to come from various government Ministries of Health or the World Health Organisation directing precautionary measures, again embedding malware
- COVID-19 tax rebate phishing lures encouraging recipients to browse to a fake website that collects financial and tax information from unsuspecting users.

Many existing organised crime groups have changed their tactics to use COVID-19 related materials on health updates, fake cures, fiscal packages, emergency benefits and supply shortages.

Typical giveaways that an email may be suspect include:

- Poor grammar, punctuation and spelling
- Design and quality of the email isn't what you would expect
- Not addressed to you by name but uses terms such as "Dear colleague," "Dear friend" or "Dear customer"
- Includes a veiled threat or a false sense of urgency
- Directly solicits personal or financial information.

Of course if it sounds too good to be true, it probably is.

The response

There are some key steps you should take to reduce the risk to your organisation and your employees, particularly as you move to remote working:

- Raise awareness amongst your team warning them of the heightened risk of COVID-19 themed phishing attacks
- Share definitive sources of advice on how to stay safe and provide regular communications on the approach your organisation is taking to the COVID-19 pandemic
- Make sure you set up strong passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access

- Provide remote workers with straightforward guidance on how to use remote working solutions including how to make sure they remain secure and tips on the identification of phishing
- Ensure that all provided laptops have up to date anti-virus and firewall software
- Run a helpline or online chat line which they can easily access for advice or report any security concerns including potential phishing
- Encrypt data at rest on laptops used for remote working given the risk of theft
- Disable USB drives to avoid the risk of malware, offering employees an alternate way of transferring data such as a collaboration tool

Also, make sure that your finance processes require finance teams to confirm any requests for large payments during the COVID-19 pandemic. This confirmation can help to guard against the increased risk of business email compromise and CEO frauds. Ideally, use a different channel such as phoning or texting to confirm an email request.

Ensure that you apply critical security patches and update firewalls and anti-virus software across your IT estate, including any laptops in use for remote working. You should expect organised crime groups to exploit any failures in the maintenance of IT systems during this pandemic.

Make certain that you back up all critical systems and validate the integrity of backups, ideally arranging for off-line storage of backups regularly. Expect an increased risk of ransomware during the COVID-19 pandemic as organised crime groups exploit COVID-19 themed phishing.

Lastly, work with your incident and crisis management team to strive to ensure your organisation has an alternate audio and video conferencing environment available. This alternate platform will be needed if you have a ransomware incident that disrupts your IT systems. And will also provide additional redundancy if your primary conferencing provider has capacity or availability issues.

COVID-19 will drive significant changes in how you and your organisation work, stay safe and stay secure.

If you have any questions or would like additional advice, please contact us.

Contacts

Martin Tyley
Partner, UK Cyber lead
KPMG in the UK
T: +44 113 231 3934
E: martin.tyley@kpmg.co.uk

Paul Taylor
Partner, Cyber in the board room
KPMG in the UK
T: +44 207 311 2164
E: paul.taylor@kpmg.co.uk

Martijn Verbree
Partner, CORPS Cyber
KPMG in the UK
T: +44 207 311 1530
E: martijn.verbree@kpmg.co.uk

kpmg.com/uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Designed by CREATE |CRT126175