KPMG

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 there has been a rapid build-out of infrastructure by cyber criminals 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 to date 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 Government websites 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 which download malware
- Phishing emails purporting to come from various government Ministries of Health or the World Health Organization 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 team awareness warning them of the heightened risk of COVID-19 themed phishing attacks
- Share a list of legitimate sources of advice on how to stay safe and provide regular communications on the approach your organisation is taking
- Make sure you enforce strong/long passwords, and preferably two-factor authentication, for all remote access accounts; particularly for Office 365 access
- Provide remote workers with guidance on how to use approved remote working solutions securely and tips on the identification of phishing
- Ensure that all laptops have up to date anti-virus, Endpoint Detection and Response (EDR) and firewall software
- Consider running a specific helpline or online chat line which staff 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 increase 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
- Reviewing your remote access including:
  -security settings/configurations
  -ensuring approved access methods are used by staff
  -remote user lists are up to date and access privileges are appropriate
  -the level of security and operational monitoring and defined exception events are appropriate (e.g. baselines for peak usage times may differ

Also make sure that your finance processes require finance teams to put in additional measures 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 environment, 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 do 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 organization work, stay safe and stay secure.

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

Contacts

Richard Tims,Partner
KPMG New Zealand
T: +64 21 521 889
E: rtims@kpmg.xxx

Philip Whitmore,Partner
KPMG New Zealand
T: +64 21 654 846
E: pwhitmore@kpmg.xxx

home.kpmg

home.kpmg/socialmedia

Publication date: 3/19/2020